

Criminal

Investigative

Policy &

Oversight



**Evaluation of
The Criminal Investigative Environment In Which
The Defense Enrollment Eligibility Reporting System
Operates**

Report Number CIPO2000S001

January 7, 2000

**Office of the Inspector General
Department of Defense**

Additional Information and Copies

This report was prepared by the Oversight Directorate, Office of the Deputy Assistant Inspector General for Criminal Investigative Policy and Oversight, Office of the Inspector General, Department of Defense. If you have questions on this evaluation or want additional copies of the report, contact Dr. Charles P. McDowell, Program Director, at (703) 604-8769 (DSN 664-8769)

Acronyms Used in This Report

AFOSI	Air Force Office of Special Investigations
ADS	Ambulatory Data System
ASD(HA)	Assistant Secretary of Defense (Health Affairs)
AUSA	Assistant United States Attorney
CDIS	CHAMPUS Detail Information System
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CHCS	Composite Health Care System
DAS	Defense Audit Service
DCIO	Defense Criminal Investigative Organization
DCIS	Defense Criminal Investigative Service
DEERS	Defense Enrollment Eligibility Reporting System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSO	DEERS Support Office
DMDC	Defense Manpower Data Center
GAO	U.S. General Accounting Office
IG, DoD	Inspector General, Department of Defense
MCIO	Military Criminal Investigative Organization
MTF	Medical Treatment Facility
NCIS	Naval Criminal Investigative Service
OASD(HA)	Office of the Assistant Secretary of Defense (Health Affairs)
OSD(P&R)	Office of the Under Secretary of Defense (Personnel and Readiness)
RAPIDS	Real-Time Automated Personnel Identification System
SJA	Staff Judge Advocate
TMA	TRICARE Management Activity
USACIDC	U. S. Army Criminal Investigation Command
USD(P&R)	Under Secretary of Defense (Personnel and Readiness)

Criminal

Investigative

Policy &

Oversight



**Evaluation of
The Criminal Investigative Environment In Which
The Defense Enrollment Eligibility Reporting System
Operates**

Report Number CIPO2000S001

January 7, 2000

**Office of the Inspector General
Department of Defense**

Additional Information and Copies

This report was prepared by the Oversight Directorate, Office of the Deputy Assistant Inspector General for Criminal Investigative Policy and Oversight, Office of the Inspector General, Department of Defense. If you have questions on this evaluation or want additional copies of the report, contact Dr. Charles P. McDowell, Program Director, at (703) 604-8769 (DSN 664-8769)

Acronyms Used in This Report

AFOSI	Air Force Office of Special Investigations
ADS	Ambulatory Data System
ASD(HA)	Assistant Secretary of Defense (Health Affairs)
AUSA	Assistant United States Attorney
CDIS	CHAMPUS Detail Information System
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CHCS	Composite Health Care System
DAS	Defense Audit Service
DCIO	Defense Criminal Investigative Organization
DCIS	Defense Criminal Investigative Service
DEERS	Defense Enrollment Eligibility Reporting System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSO	DEERS Support Office
DMDC	Defense Manpower Data Center
GAO	U.S. General Accounting Office
IG, DoD	Inspector General, Department of Defense
MCIO	Military Criminal Investigative Organization
MTF	Medical Treatment Facility
NCIS	Naval Criminal Investigative Service
OASD(HA)	Office of the Assistant Secretary of Defense (Health Affairs)
OSD(P&R)	Office of the Under Secretary of Defense (Personnel and Readiness)
RAPIDS	Real-Time Automated Personnel Identification System
SJA	Staff Judge Advocate
TMA	TRICARE Management Activity
USACIDC	U. S. Army Criminal Investigation Command
USD(P&R)	Under Secretary of Defense (Personnel and Readiness)

EVALUATION OF THE INVESTIGATIVE ENVIRONMENT IN WHICH THE DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM OPERATES

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
PART I - INTRODUCTION	1
Background	1
Military Health Care as a Target for Fraud	1
Military Health Care System	2
Defense Enrollment Eligibility Reporting System	2
Enrollment and Eligibility Systems	3
Identification Cards	4
Enrollment Procedures and Eligibility Requirements	4
Sponsors	4
Dependents	5
Statutory and Regulatory Authority	6
Purpose of the Evaluation	6
Significance of the Evaluation	6
Scope of the Evaluation	7
Prior Reviews	7
Methodology	7
Sources of Data	8
Procedures for Collecting Data	8
Analysis of Investigative Data	9
PART II - RESULTS OF EVALUATION AND RECOMMENDATIONS	
A. Current Procedures Allow Ineligible Individuals to Retain Identification Cards That May Permit Unauthorized Access to Military Health Care for Lengthy Periods	10
Introduction	10
Issuing Identification Cards	11
Reporting Status Changes and Surrendering Identification Cards	12
Recommendation, Management Comments, and Our Response	13
B. Medical Treatment Facility Efforts to Verify Eligibility and Confiscate Identification Cards From Ineligible Individuals Are Not Fully Effective	14
Introduction	14
Military Treatment Facility Efforts to Verify Eligibility	15
Military Treatment Facility Efforts to Confiscate Identification Cards From Ineligibles	17
Administrative Recoupment Actions	18

Management Controls	18
Recommendations, Management Comments, and Our Response.....	19
C. TRICARE Does Not Have a Documented System for Developing, Referring, or Tracking Potential Ineligibility Fraud Offenses That Warrant Criminal Investigation.....	21
Developing, Referring and Tracking Investigative Cases	21
DSO Referrals to TMA	22
DSO has Implemented a Partial Solution.....	23
Contract Providers and Payment Centers.....	24
Recommendation, Management Comments, and Our Response	24
D. Most Criminal Investigations Involving Ineligibility Are Closed Without Criminal, Civil, or Administrative Remedy, and the Remainder Do Not Recover Estimated Government Losses.....	29
Introduction	29
DCIO Investigations Involving Ineligibility for Medical Care	29
Database Checks That Could Assist Investigations	30
MCIO Access to Databases	32
Recommendation, Management Comments, and Our Response	32
 APPENDIX A - STATUTORY AND REGULATORY AUTHORITIES	
APPENDIX B - RELEVANT PRIOR REPORTS AND FINDINGS	
APPENDIX C - SITES VISITED DURING THE EVALUATION	
APPENDIX D - DCIO CRIMINAL INVESTIGATIONS INVOLVING INDIVIDUALS INELIGIBLE FOR MILITARY HEALTH CARE	
APPENDIX E - MANAGEMENT COMMENTS	
APPENDIX F - REPORT DISTRIBUTION	

EVALUATION OF THE INVESTIGATIVE ENVIRONMENT IN WHICH THE DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM OPERATES

EXECUTIVE SUMMARY

INTRODUCTION

We began this evaluation in response to correspondence from the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). The ASD(HA) was concerned that the Military Criminal Investigative Organizations (MCIOs)¹ were not investigating cases in which individuals used false documentation to obtain identification cards needed to access military benefits and privileges. In performing preliminary research on the ASD(HA) concerns, however, we determined that the MCIOs generally were not notified when an ineligible individual was suspected of obtaining or using an identification card. Our overall objective for the evaluation, therefore, was expanded to encompass whether the Department of Defense (DoD) is effective in preventing, detecting, and investigating instances in which ineligible individuals obtain identification cards, and the benefits they receive from using these cards. We announced this evaluation on March 13, 1997, and conducted our primary fieldwork between July 30, 1997, and February 28, 1998. We conducted additional fieldwork in January 1999. On June 10, 1999, we issued this report in draft form for management comments.

MANAGEMENT COMMENTS

On September 13, 1999, we received comments from the Office of the Under Secretary of Defense (Personnel and Readiness) (OUSD(P&R)). OUSD(P&R) concurred with some of our recommendations, but nonconcurred with others. OUSD(P&R) also stated concerns about completeness and accuracy in some sections of the draft report. OUSD(P&R)'s comments are reproduced as Appendix E.

Generally, the OUSD(P&R) nonconcurrences with individual recommendations (B.2., C.1., and D.1.) were based largely on one of the following positions:

¹ The MCIOs are the U.S. Army Criminal Investigation Command (USACIDC), the Naval Criminal Investigative Service (NCIS), and the Air Force Office of Special Investigations (AFOSI). The MCIOs, together with the Defense Criminal Investigative Service (DCIS), the IG, DoD, criminal investigative arm, collectively are known as the Defense Criminal Investigative Organizations (DCIOs).

- the recommendation should be directed to the Uniformed Services, since the Uniformed Services are responsible for determining eligibility for military health care and for terminating eligibility when an individual no longer qualifies for treatment; and
- under the terms of a Memorandum of Understanding, the Defense Criminal Investigative Service, not the Military Criminal Investigative Organizations, has lead agency responsibility for fraud involving the TRICARE Program.

The OUSD(P&R) comments are addressed in detail in this final report. For the reasons set forth in this report, we have not accepted the OUSD(P&R) bases for nonconcurring and have reaffirmed our Recommendations B.2., C.1., and D.1. We have, however, modified Recommendation D.1. to include Operation Mongoose databases among those the Military Criminal Investigative Organizations should check when investigating beneficiary medical fraud. We have also modified the final report where appropriate to address certain OUSD(P&R) concerns about completeness and accuracy in the draft report.

EVALUATION RESULTS

We were unable to determine, beyond the cases actually investigated by the MCIOs, the extent to which the DoD has a problem with ineligible individuals using the military health care system. As a result, we were also unable to determine the unauthorized costs that DoD incurs due to ineligible individuals using the military health care system. These determinations were not possible because the Office of the Assistant Secretary of Defense (Health Affairs) (OASD(HA)) does not maintain records on:

- suspected ineligible individuals who seek military health care;
- suspected ineligible individuals who are denied military health care;
- suspected ineligible individuals who are identified as actually ineligible after they obtain military health care;
- administrative actions undertaken to address ineligibility or unauthorized health care costs;
- suspected ineligibility cases referred for criminal investigation; or
- outcomes of criminal investigative case referrals.

This situation exemplifies an overall condition in which the DoD does not have an effective program to prevent, detect, or investigate ineligibility health care fraud.

Furthermore, when potential ineligibility fraud cases are investigated, the investigations generally do not result in criminal, civil, or administrative remedies. During 1995 through 1997, DoD criminal investigative organizations investigated

81 cases that involved potentially ineligible individuals receiving military health care.² At the time of our primary fieldwork, 74 of these investigations had been completed, and the cases had been closed. Forty nine (66 percent) of the closed cases were declined for prosecution and/or were closed without remedy, generally because prosecutors determined the estimated Government losses were too small to warrant prosecution, or because the investigations did not establish criminal intent. Although the remaining investigations (34 percent) produced an array of results, the monetary recoveries amounted to only about 5 percent of the estimated Government losses.

Overall, we identified the following conditions that warrant management attention and corrective action:

- Current procedures allow ineligible individuals to retain identification cards that may permit unauthorized access to military health care for lengthy periods.
- Medical treatment facility efforts to verify eligibility and confiscate identification cards from ineligible individuals are not fully effective.
- The TRICARE Management Activity does not have a documented system for developing, referring, or tracking potential ineligibility fraud offenses that warrant criminal investigation.
- Because most criminal investigations do not result in criminal, civil, or administrative remedies and those that do only recover a minor portion of the estimated Government loss, OASD(HA) must aggressively pursue administrative recoupment actions to address potential ineligibility medical fraud. If not, most unauthorized cost that DoD incurs from ineligibility medical fraud will not be recovered.

SUMMARY OF RECOMMENDATIONS

We recommend the following corrective or improvement actions:

- The Under Secretary of Defense (Personnel and Readiness), through the Joint Uniformed Services Personnel Advisory Committee, establish time limits for sponsors to (1) report a change in eligibility status for their dependents, and (2) surrender a dependent's identification card when the dependent becomes ineligible for military benefits and privileges, and adopt these time limits in appropriate policy.
- The ASD(HA) direct medical treatment facility commanders to comply with existing policy that requires:
 - 100 percent eligibility checks using the Defense Enrollment Eligibility Reporting System prior to treating military personnel or their dependents;

² Individual OASD(HA) medical facilities or medical personnel were the sources of allegations for 27 (33 percent) of these investigations (See Appendix D). These cases, however, did not constitute investigative case referrals where OASD(HA) had identified actual or potential ineligibility and referred the matter for criminal investigation.

- confiscating identification cards from ineligible individuals who seek military health care and forwarding those cards to local authorities; and
- initiating administrative recoupment actions for cost incurred when suspected ineligible individuals obtain unauthorized military medical benefits.

- The ASD(HA) (1) require the TRICARE Management Activity to implement an aggressive management control plan with fraud indicators that helps detect ineligible individuals who apply for and receive medical care through TRICARE, and (2) consider making this plan part of the TRICARE Management Activity's Annual Statement of Assurance submitted in accordance with DoD Directive 5010.38, "Management Control Program," August 26, 1996.

- The Director, TRICARE Management Activity, with input from the MCIOs, implement a system for developing, referring, and tracking cases that involve military health care given to suspected ineligible recipients. This system should include procedures and timelines for pursuing administrative remedies in cases determined not to warrant criminal investigation and prosecution. It should also include procedures and timelines for pursuing administrative remedies in cases referred for criminal investigation, but ultimately not prosecuted, unless a determination is made that an administrative recovery is not appropriate.

- The Director, TRICARE Management Activity, arrange for the Military Criminal Investigative Organizations to receive access to and system training on the CHAMPUS Detail Information System to aid their military health care investigations.

- The MCIOs implement procedures that ensure their criminal investigators who conduct military health care investigations check all relevant databases in determining the breadth of criminal conduct involved and the potential overall loss to the Department of Defense.

EVALUATION OF THE INVESTIGATIVE ENVIRONMENT IN WHICH THE DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM OPERATES

PART I - INTRODUCTION

BACKGROUND

One of the most significant benefits of military service is the broad-based, low-cost health care provided to active duty personnel, retirees, and their families. Although providing health care to military member families (dependents) dates to the American Revolution, the concept was not formalized until 1884, when Congress directed that "... medical officers of the Army and contract surgeons shall whenever possible attend the families of the officers and soldiers free of charge." Over the ensuing years, the scope of medical care provided to military members and their dependents continued to increase. Currently, health care treatments that would be prohibitively expensive if paid out of pocket, including organ transplants and hospice care, are covered by military health care services. In Fiscal Year (FY) 1997, the military health care system served 8.2 million people and cost \$15.7 billion, an amount equal to 6.2 percent of the Defense budget.

Military Health Care as a Target for Fraud

The military health care system has continued to be an attractive target for fraud. Because access to low- or no-cost medical care results in substantial monetary savings to patrons, use by unauthorized individuals has been a continuing DoD problem that has been reported in numerous audits and inspections. However, based on current OASD(HA) recordkeeping, it is not possible to estimate how many ineligible individuals actually receive military health care, or the resulting cost to DoD.³

MILITARY HEALTH CARE SYSTEM

DoD has continued to search for ways to improve access to quality medical care while controlling costs. In the late 1980s, DoD conducted several demonstration projects

³ For medical fraud generally, the United States Chamber of Commerce estimates that, on a national basis, up to 20 percent of all health care claims are fraudulent. According to these estimates, health-care providers commit 65 percent to 75 percent of the total fraud, beneficiaries commit 15 percent to 35 percent, and insurer employees commit 10 percent.

to evaluate alternative health care delivery approaches. Based on these projects, and in response to requirements in the FY 1994 Appropriations Act, DoD adopted TRICARE as its managed health-care program.⁴ TRICARE was designed to:

- ensure high-quality, consistent medical care while preserving choices as to the medical provider used;
- improve access to health care; and
- contain costs.

At the time of our fieldwork, TRICARE was being implemented nationally.

The Under Secretary of Defense (Personnel and Readiness) (USD(P&R)), through the ASD(HA), is responsible for the TRICARE program. The ASD(HA) has established 11 health service regions and exercises authority, direction, and control over TRICARE and individual medical treatment facilities (MTFs) in these regions. In each region, a military health care administrator, supported by a joint-Service staff, is lead agent for coordinating all health care services. These regional staffs are responsible for medical services provided at 115 hospitals, 471 clinics, and through various private medical practitioners who serve TRICARE patients on a contract basis. The TRICARE Management Activity (TMA), located in Denver, Colorado, is responsible for program oversight. TMA is also responsible for supporting contractors that provide health care to military members and their dependents.

DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM (DEERS)

Congressional concern over military health care fraud and abuse, and the need for improved military health resources management, led DoD to develop and implement DEERS beginning in 1979.⁵ DEERS is a computer-based, on-line system that contains personal, Service-related eligibility and demographic data on all Service members, retirees, and their family members. DEERS also contains the information needed to determine an individual's eligibility for military benefits, including health care, commissary, and exchange privileges. The DEERS database contains information on over 17.2 million people, including 6.5 million military members (sponsors)⁶ and 10.7 million dependents. Individuals with records in the database include:

⁴ The previous Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) became one optional medical approach available under TRICARE. On February 10, 1998, the Office of Civilian Health and Medical Program of the Uniformed Services (OCHAMPUS) became the TRICARE Management Activity. For purposes of this report, we refer to the current program and organizational elements.

⁵ Although created to support the military health system, DEERS has been expanded to include eligibility status for other military privileges. The system has also been expanded to interface with other DoD systems and programs.

⁶ In the health care community, a military member is generally referred to as the sponsor, since family members would not be entitled to services except for the military member's status.

-
- active duty military personnel;
 - retired military personnel;
 - members of the military reserve components;
 - overseas civil service personnel who support the Armed Forces and their dependents;
 - dependents of active, retired and reserve personnel;
 - dependents of military members who died on active duty or after retirement;
 - members of the United States Coast Guard; and
 - members of the Commissioned Corps of the United States Public Health Service and the National Oceanic and Atmospheric Administration.⁷

USD(P&R) is also responsible for DEERS operations. The Defense Manpower Data Center (DMDC), which reports to USD(P&R), is systems administrator for DEERS. The DEERS policy office is located in Rosslyn, Virginia. The DEERS Support Office (DSO) is located in Seaside, California.

Enrollment and Eligibility Systems

DEERS is both an *Enrollment System* and an *Eligibility System*. The *Enrollment System* combines dependent data with sponsor data. This system generates individual records for the *Eligibility System* and is used to produce management and demographic reports. Based on DEERS information, Service members, their eligible dependents, and other eligible individuals are given distinctive identification cards. These identification cards establish each individual's eligibility for specific military benefits and privileges. The *Eligibility System* identifies each individual's eligibility status.

Identification Cards

Military members and their dependents are issued identification cards to identify them as individuals eligible to receive military benefits and privileges. Prior to 1985, military identification cards were produced manually, with the issuing official typing the required information in the appropriate blocks. This process was both error-prone and

⁷

The United States Public Health Service, Department of Health and Human Services, and the National Oceanic and Atmospheric Administration, Department of Commerce, each has a commissioned corps with officers who wear uniforms similar to Navy uniforms and who receive pay and benefits identical to members of the Armed Forces. These two corps are sometimes referred to as "Uniformed Services," as opposed to "Armed Forces," because their respective missions are typically more scientific and technical than military in nature. Under agreement with the Secretary of Defense, Uniformed Service members receive military-related benefits.

time consuming. In 1985, DoD began implementing the Real-Time Automated Personnel Identification System (RAPIDS). Because RAPIDS produced computer-generated identification cards, it was designed to reduce errors and the time required to prepare the cards. In addition, RAPIDS had the added benefit of improving information reliability in the DEERS database. At the time of our fieldwork, DMDC was implementing RAPIDS 5.0 worldwide.

Enrollment Procedures and Eligibility Requirements

Enrollment procedures and eligibility requirements are set forth in DoD Instruction (DoDI) 1000.13, “Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,” December 5, 1997. A Joint Service and Uniformed Services Instruction, “Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel,” July 14, 1998 (hereafter referred to as the Joint Instruction),⁸ details procedures and eliminates many Service-peculiar requirements. In most instances, this Instruction provides for “cross-servicing” military members.⁹ The enrollment process is summarized below.

Sponsors. Sponsor information is added to DEERS at the point of entry into military service. At the same time, the sponsor is given a DD Form 2, “U.S. Armed Forces Identification Card.” Prior to late 1997, active duty and reserve members were given different color-coded cards, making it easy to distinguish their status and, thereby, their different entitlements to military benefits and privileges. Some reservists and congressional representatives, however, perceived the different identification card colors as a barrier to achieving a fully integrated force. USD(P&R), therefore, decided that active duty and reserve personnel would be issued the same color cards. In announcing this decision on December 4, 1997, USD(P&R) emphasized that, while the color of the card had changed for reservists, the benefits, entitlements and DEERS update requirements remained the same.

The Military Departments automatically forward updated DEERS information on their active duty members, including changes in unit assignment and pay grade, as well as information on discharges, dismissals, separations, and retirements. When a military member retires, a new color-coded card is issued. Active duty, retiree, and reservist identification cards are valid indefinitely.

⁸ This instruction was issued by order of the Secretaries of the Army, Navy, Air Force, Transportation (for the Coast Guard), Commerce (for the National Oceanic and Atmospheric Administration), and Health and Human Services (for the Public Health Service), and the Commandant of the Marine Corps. It is identified as: Air Force Instruction 36-3026(I); Army Regulation 600-8-14; BUPERS Instruction 1750.10A, Change 1; Marine Corps Order P5512.11B, Change 1; Commandant Instruction M5512.1; Commissioned Corps Personnel Manual 29.2, Instructions 1 and 2.

⁹ The cross-servicing concept altered the perception that a Military Department generally served only its own members. Cross servicing allows a Military Department to serve any military member without regard to the member’s Military Department.

Dependents. Sponsors are responsible for enrolling their dependents in DEERS. Local military installation personnel accomplish these enrollments using DD Form 1172 (DD 1172), “Application for Uniformed Services Identification Card DEERS Enrollment.” The DD 1172 requires biographic and relational information that must be supported with official documentation, such as a marriage license, birth certificate, or court order. The sponsor must sign the DD 1172, certifying under penalty of law that the information furnished is correct. An issuing or verifying official¹⁰ then enters the necessary information into DEERS using dedicated computer terminals. Based on the DD 1172 information, each eligible dependent is issued an identification card.

The sponsor is also responsible for (1) notifying DEERS when an eligible dependent’s status changes, and (2) returning a dependent’s identification card when the dependent is no longer eligible for military benefits and privileges. In addition, the sponsor must submit documentation supporting a request for status change. For example, when adding a child as a dependent, a sponsor must present a birth certificate, adoption document, or court order. Similarly, when deleting a spouse from eligibility following a divorce, the sponsor must provide a copy of the divorce decree. Only a verifying or issuing official may make an addition to the DEERS database; however, either a verifying/issuing official or DSO may delete DEERS data. Although an individual’s (sponsor or dependent) status may change in the *Eligibility System*, the individual is never deleted from the *Enrollment System*. Dependent identification cards must be renewed every 4 years or when a change in status occurs.

In FY 1996, daily activity in DEERS totaled nearly 732,000 actions, including over 300,000 sponsor batch updates, nearly 200,000 TRICARE inquiries, about 125,000 personnel inquiries, and over 20,000 on-line address updates.

STATUTORY AND REGULATORY AUTHORITY

The statutory and regulatory authorities covering eligibility for military benefits and the penalties for misusing or abusing them are listed in Appendix A.

PURPOSE OF THE EVALUATION

On October 23, 1996, the IG, DoD, issued “Revised Interim Guidance for Criminal Investigations of Fraud Offenses Jurisdiction.” After reviewing the Revised Interim Guidance, on January 10, 1997, the ASD(HA) wrote to the IG, DoD, advising that there was “... no evidence that the Military Criminal Investigative Organizations

¹⁰ Under existing policy, an issuing or verifying official is a person who is a military member in an E-4 or higher grade, or a civilian employee in a GS-4 or higher grade.

investigate the submission of false documents to obtain dependent identification cards.” The ASD(HA) noted that the TRICARE Management Activity was receiving approximately 100 letters a month from the DEERS Support Office requesting recoupment actions.¹¹ According to ASD(HA), these letters identified individuals whom the appropriate Military Department had determined were ineligible for military benefits, but whom DEERS incorrectly listed as eligible for military health care. The ASD(HA) indicated that the MCIOs were not requesting claims histories or other documentation needed to determine whether claims submitted to TRICARE were valid.

In performing preliminary research on the ASD(HA) concerns, we determined that the MCIOs generally were not notified when an ineligible individual was suspected of obtaining or using an identification card. Our primary objective for this evaluation, therefore, was expanded to encompass overall DoD effectiveness in preventing, detecting, and investigating ineligible military dependents that obtain identification cards, and then improperly derive benefits from using them.

SIGNIFICANCE OF THE EVALUATION

The universe of individuals receiving military health care benefits is extensive, consisting of 8.2 million people in FY 1997. The portion of this total represented by individuals who are ineligible for the benefits they receive, or the value of those benefits, cannot be estimated reasonably based on current OASD(HA) recordkeeping.

SCOPE OF THE EVALUATION

We limited our evaluation to members of the Armed Forces and their dependents. Our evaluation did not include Uniformed Services personnel from the Coast Guard, the Public Health Service, or the National Oceanic and Atmospheric Administration. We also limited our evaluation to transactions taking place in the Continental United States and those involving family members suspected of obtaining and using dependent identification cards improperly to obtain military health care.¹²

¹¹ Between mid-1994 and December 1996, DSO sent TMA letters concerning 7,496 individuals who lost eligibility for military-related benefits during some period of time. These letters are discussed in greater detail later in this report.

¹² Identification cards may also be used improperly to gain access to military commissaries and exchanges. Although we visited some of these facilities and interviewed program officials, we are excluding this topic from our report because the fraud aspects are inconsiderable. Even though a patron with an invalid identification card may gain access to these facilities, the individual must still pay for the goods and services obtained, albeit presumably at a savings over civilian stores. This is not the case with health care.

PRIOR REVIEWS

The U.S. General Accounting Office (GAO) and the OIG, DoD, have both conducted significant audits and other work related to identification cards and their improper usage. Beginning in the 1970s, these agencies reported on weaknesses in issuing and recovering identification cards, as well as on ineligible persons who used these cards to obtain unauthorized military health benefits. These reports identified various systemic problems and estimated that, as a result, millions of dollars were misspent annually. Some previous reports pointed out that lost or stolen identification cards were easily replaced, and manually produced cards were easy to alter and counterfeit. Appendix B identifies the relevant reports and summarizes their major findings.

METHODOLOGY

This evaluation sought to assess several interrelated areas:

- how ineligible individuals are able to obtain or retain identification cards;
- how ineligible individuals are able to enroll in DEERS;
- how ineligible individuals with identification cards are detected;
- how the MCIOs learn about fraudulent identification card activity and their responses to the problem;
- the types of punishment, including administrative actions, imposed on sponsors and dependents for misusing identification cards; and
- the processes and procedures used to prevent or deter fraudulent enrollments.

Sources of Data

We obtained and reviewed information from the following sources:

- official TMA records;
- official DMDC records and statistical data;
- previous audit and other reports addressing military health care; and
- DCIO investigative data.

We also conducted site verification visits and evaluated eligibility data at multiple field locations.

Procedures for Collecting Data

To determine how ineligible individuals obtain and use identification cards, and how their actions are discovered and investigated, we evaluated the processes used, beginning with those for issuing identification cards and continuing through subsequent investigations and prosecutions (if any). We also examined individual steps in the processes, from the issuing or verifying official's actions in issuing the identification card to an administrative or judicial remedial action taken against the offender.

Various statutory and regulatory guidance prescribe the requirements that govern determining eligibility and issuing identification cards that permit military health care, and conducting investigations when suspected ineligible individuals obtain such care (see Appendix A). Data obtained from DMDC, TRICARE, Service personnel offices, MTFs, and the DCIOs were used to assess how the system works from application to redress. Several sites were selected for assessing program implementation and management controls. These sites were chosen based on information obtained from MCIO, DEERS, TRICARE, and Service personnel officials. In identifying specific sites to visit, we employed the following criteria for assessing their evaluation potential:

- The number of military trainees served. We assumed that a larger trainee volume would involve a larger flow of dependents and, therefore, a larger potential for ineligible dependents to be processed and receive identification cards inappropriately.
- Whether the installation served multiple Services. Multiple Service presence would increase the number of identification card issuing offices and MCIOs involved in investigations.
- Whether the installation was located in an isolated area. If so, military members would have to rely on off-site medical care and investigative support could be limited.

We conducted site visits at 12 military installations: 3 Army; 2 Navy; 1 Marine Corps; 5 Air Force; and 1 joint reserve active duty base. We interviewed personnel officers, issuing and verifying officials, MTF staff, judge advocates, and MCIO representatives.

We also interviewed members of the Service Personnel Advisory Committee, since this committee serves as policy advisor to the USD(P&R) on personnel matters. In addition, we visited or contacted officials at OASD(HA), DMDC, DSO, TMA, three medical health service regional offices, three TRICARE contractors, and one TRICARE payment center. The sites that we visited or contacted are identified in Appendix C.

Analysis of Investigative Data

We analyzed data from 81 criminal investigations involving ineligibility that the DCIOs conducted during 1995 through 1997. Of this total, USACIDC conducted 37 for

the Army; NCIS conducted 21 for the Navy and Marine Corps; AFOSI conducted 13 for the Air Force; and DCIS conducted 10 for the Services and Defense Agencies.

EVALUATION OF THE INVESTIGATIVE ENVIRONMENT IN WHICH THE DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM OPERATES

PART II - RESULTS OF EVALUATION AND RECOMMENDATIONS

A. CURRENT PROCEDURES ALLOW INELIGIBLE INDIVIDUALS TO RETAIN IDENTIFICATION CARDS THAT MAY PERMIT UNAUTHORIZED ACCESS TO MILITARY HEALTH CARE FOR LENGTHY PERIODS

The issuing and verifying officials that we visited followed proper procedures in processing requests and issuing identification cards. However, personnel at only one site took a proactive approach by specifically outlining sponsor responsibilities and liabilities, and thoroughly questioning applicants concerning their sponsor relationships. Such an approach helps to determine whether dependents are eligible for military benefits and privileges before identification cards are issued or renewed. In addition, although required to do so, sponsors had not recovered identification cards from their former spouses in any divorce case that we reviewed. Furthermore, as discussed in Part II, Section B of this report, MTFs generally were not effective in confiscating identification cards from ineligible individuals. While current recordkeeping precluded us from fully assessing the resulting impact, it is clear that this condition enabled ineligible individuals to retain identification cards that would allow them to continue receiving military benefits and privileges after they had become ineligible. It is also clear that, in some cases, this condition continued for many years.

Introduction

DoDI 1000.13 outlines policy, procedures, and responsibilities for issuing identification cards. The Joint Instruction (see Footnote 8), which implements DoDI 1000.13, combines all Service-unique regulations and instructions into a comprehensive guidebook for verifying officials. It also outlines the DEERS enrollment process, and provides step-by-step procedures for determining eligibility, completing the DD 1172, and issuing the identification card.

Section 3.1. of the Joint Instruction prescribes sponsor responsibilities as follows:

“3.1.1. Active, Retired, Guard, and Reserve sponsors should

advise the nearest uniformed service issuing activity about any changes to dependent data that affect eligibility to a DD Form 1173 or DD Form 1173-1.

3.1.2. Provide documentation to update the DEERS for dependents no longer entitled to benefits and privileges (for example, final divorce decree, child's marriage certificate, etc.)

3.1.3. Retrieve ID cards from dependents no longer eligible and surrender the cards to the nearest ID card issuing activity.”

Sponsor responsibilities are also outlined in Sections III and VIII of the DD 1172. When the sponsor signs the DD 1172, he or she:

- attests that the information is true and accurate;
- assumes responsibility for reporting changes in dependent status;
- agrees to surrender the card when appropriate; and
- subjects himself or herself to fines up to \$10,000 or imprisonment up to 5 years (or both) for making false statements.

Neither this nor other DoD policy, however, establishes a deadline or timeframe for reporting a status change, or for surrendering an identification card when an individual becomes ineligible for military benefits and privileges.

Issuing Identification Cards

We interviewed issuing and verifying officials and observed enrollment procedures at 11 issuing offices. These officials performed DEERS enrollment actions that resulted in identification card issuances ranging from a few hundred to over 3,000 per month. Approximately 50 percent of these actions involved dependents.

Each issuing and verifying official that we visited followed proper procedures in accepting and processing DD 1172s, and in issuing the identification cards. When lines were left blank, they requested additional information. For initial enrollment requests, they requested supporting documentation. However, personnel at only one site took a proactive approach. Issuing officials at this site specifically outlined sponsor responsibilities and liabilities, and thoroughly questioned applicants concerning their sponsor relationships. The verifying official at this site advised that she, to discourage ineligible enrollments, encouraged her issuing officials to fully, but politely, question all enrollment applicants and remind sponsors of their responsibilities and legal liabilities. However, none of the issuing or verifying officials tracked the number of identification

cards that they denied based on ineligibility.¹³ Therefore, it was not possible to quantify or reasonably estimate the number of potential ineligible enrollments that the one issuing office dissuaded with its efforts, or the number that could be prevented overall through such efforts by issuing and verifying officials generally.

Reporting Status Changes and Surrendering Identification Cards

As noted above, sponsors are responsible for reporting changes in dependent status and surrendering identification cards when their dependents become ineligible. According to both personnel office and DEERS officials, however, some sponsors “ignore or forget” their responsibilities, especially in divorce situations. According to these officials, friendly divorces often result in a sponsor continuing to enroll a former spouse rather than providing for private health care. Similarly, hostile divorces often result in former spouses refusing to return their identification cards. Since states do not require a marriage certificate to be altered when a divorce occurs, the marriage certificate can still be used as supporting documentation to obtain an identification card after a divorce is final. These cards, and the underlying ineligible DEERS enrollments, may not be detected until the sponsor remarries and attempts to enroll the new spouse.

We analyzed 81 ineligibility cases that the DCIOs investigated (see Appendix D). We also discussed dependent update requests with DSO officials. Thirty (37 percent) of the 81 DCIO investigations involved divorces that had not been reported to DEERS. Fifteen of the divorces had been final for at least a year, and of those, 9 had been final from 4 years to 26 years.¹⁴ In these nine cases, the identification cards had been renewed at least one time after the divorces became final, some with the sponsor’s signature and some with the former spouse’s signature. In the latter cases, the former spouses used their expiring identification cards as the basis for obtaining new cards.

The sponsor had not recovered the identification card from the former spouse, as required, in any of the 30 divorce cases that we reviewed. In nearly every case, the sponsor claimed that no one had explained the reporting requirements or when status changes must be reported. By reporting the divorce after a new marriage, without regard to the timeframe, the sponsors believed they had fulfilled their responsibilities. However, during the intervening time, ineligible former spouses continued to have nominally valid identification cards that they could use to receive military health care benefits.

RECOMMENDATION, MANAGEMENT COMMENTS, AND

¹³ They did track the number of cards issued and the number of updates accomplished, but these statistics were not helpful in assessing ineligibility determinations.

¹⁴ Overall, 9 (30 percent) had been final for less than a year, 15 (50 percent) had been final for a year or more, and we could not determine time for the remaining 6 (20 percent).

OUR RESPONSE

A. We recommend that the Under Secretary of Defense (Personnel and Readiness), through the Joint Uniformed Services Personnel Advisory Committee:

- 1. establish time limits for sponsors to report a change in eligibility status for their dependents, and surrender a dependent’s identification card when the dependent becomes ineligible for military benefits and privileges; and**
- 2. adopt these time limits in appropriate policy.**

OUSD(P&R) concurred and advised that the Joint Uniformed Services Personnel Advisory Committee had been asked to establish the time limits.

The comments are responsive to our recommendation. In responding to the final report, OUSD(P&R) should provide an estimated completion date for adopting the time limits in its policy.

B. MEDICAL TREATMENT FACILITY EFFORTS TO VERIFY ELIGIBILITY AND CONFISCATE IDENTIFICATION CARDS FROM INELIGIBLE INDIVIDUALS ARE NOT FULLY EFFECTIVE

The Assistant Secretary of Defense (Health Affairs) and the Military Departments all have policies requiring medical treatment facilities and TRICARE providers to verify eligibility when an individual requests medical services, and the locations we visited all had established procedures to effect this policy. The policies and procedures were not applied consistently, however, and were not fully effective in detecting ineligible individuals. In addition, even though the Joint Instruction authorizes confiscating identification cards from ineligible individuals, only Navy policy includes actual guidance on confiscation, and this guidance does not specifically require the action. As a result, the policies and procedures do not ensure that identification cards are confiscated from ineligible individuals, thereby allowing the individuals to retain them for future unauthorized use.

Introduction

HA Policy 97-057, “Policy for Defense Enrollment Eligibility Reporting System (DEERS) Eligibility Checking Requirements,” July 11, 1997, provides:

“Effective October 1, 1997, eligibility checks will be performed prior to each outpatient healthcare evaluation at ... [medical treatment] facilities with the capability for electronic validation. The check will be made automatically between the Ambulatory Data System, the Composite Health Care System and DEERS, transparent to the user unless the system reports an eligibility issue requiring intervention and patient notification...Current policy requiring 100 percent checks of all patients being admitted to ... hospitals, all prescriptions written by civilian providers, and all nonactive duty dental visits will continue.”

Each Military Department also requires eligibility verification. For example, Air Force Instruction 41-115, “Authorized Health Care and Health Care Benefits in the Military Health Services System (MHSS),” July 25, 1994, refers to eligibility verification as a two-step process. The first step is twofold: requiring patients to present valid identification cards; and requiring MTF staff members to ensure all patients, including those in uniform, present valid identification prior to receiving routine care, or ancillary or administrative services. The second step requires MTF staff members to verify a patient’s eligibility status in DEERS. The instruction also requires each MTF to have

written instructions on how to handle patients with questionable eligibility. When this verification process results in questionable eligibility, routine care is supposed to be denied.

MTF Efforts to Verify Eligibility

We visited 3 health service regions and 8 MTFs, ranging from clinics to 500-bed hospitals, and reviewed their processes and procedures for detecting and deterring ineligible individuals from using the facilities. All hospitals and clinics use the Composite Health Care System (CHCS), which interfaces with DEERS,¹⁵ to schedule medical appointments and hospital admissions. They also use CHCS to track scheduled/walk-in appointments, emergency treatments, hospital admissions, and pharmacy prescriptions. When a user enters a patient name in CHCS, the system shows when a DEERS check was last performed on the patient. If a DEERS check has not been performed, or if the prior DEERS check is more than 5 days old, CHCS will automatically perform a new DEERS check and advise the user on current patient eligibility. If the user is scheduling a medical appointment or hospital admission more than 5 days in the future and the DEERS check will no longer be valid when the appointment or admission occurs, CHCS will also provide for an automatic update, generally 72 hours before the scheduled appointment or admission. However, the updates are “batch” reports¹⁶ and MTF personnel must review the batch reports to determine eligibility at the time of the appointment or admission. In addition, to prevent system problems from delaying or preventing patient scheduling, CHCS users have the option to bypass the automatic DEERS check capability and “batch” report all DEERS checks.

CHCS users at the hospitals and clinics that we visited generally opted to bypass the automatic DEERS checking capability. In fact, they appeared to view the batch report capability as the automatic system capability.¹⁷ As a result, they were performing immediate, on-screen DEERS checks only as shown in Table 1.

¹⁵ Some facilities do not interface with “native DEERS” and, instead, access DEERS download data. Thus, while all of the facilities have direct DEERS interfaces, some do not have real-time DEERS access.

¹⁶ CHCS has the capability to accumulate, or batch together, requests for DEERS checks and then, at a designated date and time, produce a printed report showing results for the individual requests included in the batch.

¹⁷ This may have been because slower MacData servers were supporting CHCS at the time of our fieldwork. Even though these servers have now been replaced, our recent follow-up contacts with the facilities indicate that this situation has not changed and CHCS’ automatic eligibility checking capability is still not being utilized fully.

Table 1
Medical Treatment Facility DEERS Checks

Type of Medical Service	No. of Facilities	No. of Facilities Checking DEERS
Scheduled/Walk-in Appointment	8	1
Emergency Treatment	8	1
Hospital Admission	6 *	2
Pharmacy	8	8

* Two of the eight facilities were clinics, not hospitals.

As Table 1 shows, the pharmacy operations at all eight medical facilities checked patient eligibility in DEERS. However, only one of eight hospitals or clinics (12.5 percent) checked DEERS eligibility in scheduling appointments and providing emergency treatments. Similarly, only two of six hospitals (33.3 percent) checked DEERS eligibility in admitting patients. Generally, except for the pharmacy operations, the facilities relied on CHCS data, accessing DEERS only when a potential patient was new to the MTF and did not have a record on file at the facility.¹⁸ CHCS has patient information, but not time-sensitive eligibility data.

Furthermore, the one MTF that did perform routine DEERS checks instituted the practice only 6 months prior to our visit. During July 1997, that facility performed 4,376 DEERS checks and identified 136 potential ineligible (3.1 percent). During August 1997, the facility performed 7,311 DEERS checks and identified 91 potential ineligible (1.2 percent). Most of the potential ineligible had not renewed their identification cards, which had expired, and were referred to the issuing offices to request new cards. Approximately one quarter (56 individuals) of the potential ineligible the MTF identified through DEERS checks were determined to be ineligible for care in non-emergency situations and were refused treatment.

¹⁸ Two of the facilities did perform periodic, after-the-fact DEERS checks on the scheduled/walk-in appointment patients they actually served. Officials at these facilities advised that very few ineligible individuals requested care, and they were usually detected during these periodic reviews. However, policy requires the eligibility checks prior to treatment.

MTF Efforts to Confiscate Identification Cards From Ineligibles

The Joint Instruction sets forth overall policy for confiscating identification cards. According to this policy:

“1.5. ID cards are government property. Any commissioned or noncommissioned officer or military police member may confiscate an ID card that has expired, is being fraudulently used, or is presented by a person not entitled to its use...

1.5.2. Civilian employees (appropriated and nonappropriated fund) of benefits and privileges activities ... must confiscate ID cards from active duty members or from retirees or dependents of members of any service if the cards are:

1.5.2.1. Mutilated so that their use as a credential is questionable.

1.5.2.2. Expired.

1.5.2.3. Obviously altered.

1.5.2.4. Presented by an ineligible person.

1.5.3. After confiscating the ID card or if involved in a situation requiring confiscation, notify the installation security authority immediately.

1.5.4. Installation security authorities investigate confiscation cases or refer these cases to the appropriate service special agent office ... when it is warranted by circumstances or according to local procedures...

1.5.4.3. For cases involving fraud, misuse, or abuse of an ID card, prepare DD Form 1569, Incident/Complaint Report:

1.5.4.3.1. Process this form through normal investigative and administrative channels.

1.5.4.3.2. Send a copy of the completed report to the member’s commander for appropriate action...”

Each Military Department has regulatory guidance concerning eligibility verification and patient care at MTFs.¹⁹ Neither Army nor Air Force policy, however,

¹⁹ We reviewed: Army Regulation 40-3, “Medical, Dental and Veterinary Care,” February 15, 1985; Navy Medical Command Instruction 6320.3B, “Medical and Dental Care for Eligible Persons at Navy Medical Department (Continues on next page)

includes guidance on card confiscation. Furthermore, while Navy guidance indicates that an invalid card should be confiscated and forwarded to the local authorities, the guidance does not specifically require doing so.

Only two of the eight MTFs (25 percent) that we visited attempted to confiscate identification cards from individuals who could not prove eligibility or who presented an expired identification card. Staff members at these two MTFs generally telephoned their security offices upon detecting an invalid identification card. According to MTF officials, however, individuals with these identification cards usually left the area before security personnel arrived. A third MTF referred questionable cardholders to the patient affairs office. However, the director of this office stated that he seldom saw questionable cardholders “because there are many doors between the administrative desks and his office.” The director advised that only patients who are legitimately eligible, but who have not been properly included in DEERS, or who have expired identification cards, come to his office. MTF administrators, on the other hand, cited confusion over confiscation authority and insufficient Service guidance on the types of identification cards that should be confiscated as reasons for the low level of confiscation.

Administrative Recoupment Actions

Each Military Department has policy requiring MTFs to bill individuals who receive medical treatment and who are subsequently shown to have been ineligible for the treatment they received. In addition, each MTF that we visited had procedures for billing ineligible patients. However, no MTF had data showing individuals that had actually been billed, or reimbursements that had actually been received. MTF administrators advised us that no one had ever asked for data on fraudulent medical care, or the associated costs and recoupments. Therefore, they did not track these data.

Management Controls

We visited the TRICARE Management Activity, three TRICARE contractors, and one payment center to determine their respective processes for detecting ineligible individuals and for deterring them from using the TRICARE program. We found that TMA had not instituted management controls to detect and deter ineligible individuals. However, we also found that the three TRICARE contractors we visited, as well as the payment center, had controls in place and were effectively following procedures.

DoDD 5010.38, “Management Controls Program,” August 26, 1996, requires DoD components to identify weaknesses in their assessable units and submit Annual Statements of Assurance, including plans and timelines for correcting material

Facilities,” May 14, 1987; and Air Force Instruction 41-115, “Authorized Health Care and Health Care Benefits in the Military Health Services System (MHSS),” July 25, 1994.

weaknesses. TMA, through ASD(HA), submits Annual Statements of Assurance. The TMA Annual Statement of Assurance dated October 3, 1997, rated controlling fraud and abuse cases as “high,” with controls provided by in-house reviews.

TMA, with DCIS input and advice, had instituted an aggressive management control plan to detect fraudulent provider and medical institution practices. TMA and DCIS officials advised us that the fraud indicators used in this plan had been highly successful in detecting providers and institutions that committed fraud. However, a similar plan had not been instituted to assist in detecting beneficiary fraud.²⁰

RECOMMENDATIONS, MANAGEMENT COMMENTS, AND OUR RESPONSE

B.1. We recommend that the Assistant Secretary of Defense (Health Affairs) direct medical treatment facility commanders to comply with existing policy that requires:

- a. 100 percent eligibility checks using the Defense Enrollment Eligibility Reporting System prior to treating military personnel or their dependents;**
- b. confiscating identification cards from ineligible individuals who seek military medical care and forwarding those cards to local authorities; and**
- c. initiating administrative recoupment actions for cost incurred when suspected ineligible individuals obtain unauthorized military medical benefits.**

OUSD(P&R) concurred and advised that complete implementation was planned by November 1, 1999.

The management comments are responsive. In responding to the final report, OUSD(P&R) should advise whether it was able to meet the planned date.

B.2. We recommend that the Assistant Secretary of Defense (Health Affairs):

- a. require the TRICARE Management Activity to implement an aggressive management control plan with fraud indicators that helps detect ineligible individuals who apply for and receive medical care through TRICARE; and**
- b. consider making this plan part of the TRICARE Management**

²⁰

In accordance with the IG, DoD “Revised Interim Guidance for Criminal Investigations of Fraud Offenses Jurisdiction” referenced previously, the MCIOs are responsible for investigating beneficiary fraud.

Activity’s Annual Statement of Assurance submitted in accordance with DoD Directive 5010.38, “Management Control Program,” August 26, 1996.

OUSD(P&R) nonconcurred. According to OUSD(P&R):

- the Uniformed Services are responsible for determining a person’s eligibility as a TRICARE/CHAMPUS beneficiary;
- TRICARE does not have authority to determine or terminate eligibility;
- a management control program more properly lies with the Uniformed Services to ensure DEERS information is accurate and valid;
- TMA has authority to mandate that DEERS be accessed for each claim to ensure the individual is eligible for the dates of service being billed and this is currently being done;
- as indicated above (in response to Recommendation B.1.), MTFs will perform a 100 percent DEERS eligibility check for care done in the direct care system; and
- the existence and use of an accurate centralized eligibility database (DEERS) is a major fraud control tool.

OUSD(P&R) apparently misunderstood our recommendation. Our recommendation addresses a need for detecting possible beneficiary fraud, not authority for determining or terminating eligibility. Furthermore, we recommended the same approach for detecting beneficiary fraud as was already in use for detecting medical provider fraud. As discussed in the report, TMA, with DCIS input and advice, implemented a successful management control plan to detect fraudulent provider and medical institution practices. Working with the MCIOs to develop fraud indicators for beneficiary fraud and implementing a similar plan focusing on possible beneficiary fraud, as we recommended, should be similarly successful.

In addition, in the draft report, we related statements by both TMA program integrity and legal representatives, and noted that their attitudes appeared to limit actions on beneficiary fraud. In commenting on the draft report, OUSD(P&R) advised that the statements we referenced were taken out of context. According to OUSD(P&R), the statements did not relate to fraud cases, but to ID cards issued erroneously to individuals who had lost eligibility for CHAMPUS/TRICARE because they had attained eligibility for Medicare Part A, under age 65, due to disability or end stage renal disease (see Appendix E). In view of the clarification that the statements were intended to relate only to a certain type of case, we have deleted the statements and our reference to them in the final report.

C. TRICARE DOES NOT HAVE A DOCUMENTED SYSTEM FOR DEVELOPING, REFERRING, OR TRACKING POTENTIAL INELIGIBILITY FRAUD OFFENSES THAT WARRANT CRIMINAL INVESTIGATION.

The TRICARE Management Activity cannot identify the extent to which potential ineligibility cases are referred for investigation. Further, while the DEERS Support Office has begun a computer matching process that represents a good first step toward addressing ineligibility medical cases, this process is incomplete and is also based on a threshold for investigative referral that would “forgive” most ineligibility fraud. Such a result would be contrary to existing policy that requires administrative recoupment actions.

Developing, Referring and Tracking Investigative Cases

TMA publishes an annual “Chartbook of Statistics,” which includes statistics on “Fraud and Abuse Cases Finalized” in the prior fiscal year.²¹ According to these statistics, TMA finalized 235 fraud and abuse cases in FY 1994, including 68 (29 percent) beneficiary/sponsor cases. For FY 1995, TMA finalized 253 fraud and abuse cases, including 43 (17 percent) beneficiary/sponsor cases. In December 1996, during research for another proposed evaluation, we asked TMA for specific information on the 68 FY 1994 and 43 FY 1995 beneficiary/sponsor cases (111 cases in total). TMA, however, could not identify the individual cases. TMA also could not furnish information on either the dollar amounts involved or the final case dispositions.

We also asked TMA for information on additional beneficiary fraud and abuse cases. We specifically requested information on potential offenders, alleged offenses, dollar amounts involved and case status, including the case opening date, the date forwarded for investigation and the investigation closure date. In February 1997, the TMA submitted a hand-written, fragmented listing showing 66 fraud and abuse cases. Of the total, 15 cases (22.7 percent) involved possible ineligibility. The remaining 51 cases involved other health insurance coverage, drug or emergency room over-utilization, false claims, or altered receipts.

The 15 potential ineligibility cases had the following characteristics:

²¹ An example is, “CHAMPUS Chartbook of Statistics: Civilian Health and Medical Program of the Uniformed Services,” December 1995 (OCHAMPUS Guide 5400.2-CB).

- estimated Government losses (ranging from \$4,043 to \$62,584 per case) were identified for 9 cases, but estimated losses were not determined for the remaining 6 cases;
- 10 cases were awaiting action in the TMA Program Integrity Branch;
- 1 case had been closed following a criminal investigation and prosecution that resulted in a conviction;
- 1 case had been closed without a criminal investigation following an administrative recoupment action; and
- 3 cases had been referred to DCIS for criminal investigation in accordance with a Memorandum of Understanding between OASD(HA) and DCIS then in existence.²²

In September 1997, we asked the Program Integrity Branch for an updated case listing, including new potential cases. The response, which again was handwritten and fragmented, included 7 additional potential ineligibility cases, increasing the total to 22 cases.

In December 1996 and October 1997, we visited TMA to review the processes used to develop, refer for investigation, and track potential eligibility fraud cases. The TMA, however, did not have a documented process for these purposes.²³ Although TMA Program Integrity Branch officials estimated that TMA was processing approximately 1,000 possible fraud cases, they could not furnish actual statistics, identify the cases involving possible beneficiary fraud, or share case status information. According to the officials, TMA did not have or plan to have a database to track its fraud case developments or investigative referrals.

DSO Referrals to TMA

As noted previously, ASD(HA) advised that the DEERS Support Office was sending the TRICARE Management Activity monthly letters identifying individuals who had become ineligible for military benefits and privileges. DSO began this practice in mid-1994, so TMA could determine whether an ineligible individual had received military medical care during the month.²⁴ If so, TMA could then decide how to seek monetary recovery from the ineligible individual. From mid-1994 through the end

²² See Appendix B, page B-2, final bullet.

²³ Several TMA employees were responsible for individual cases and maintained files in their work areas. They could not, however, readily identify or locate individual files, or relate specific case data. The procedures in effect did not constitute an effective, documented process that could be used and relied upon for thoroughness, completeness, or consistency.

²⁴ DSO discontinued sending the monthly letters after December 1996, because it was not receiving any feedback.

of 1996, DSO forwarded 7,496 such letters to TMA, but did not receive any feedback on the dispositions.

At the time of our research visit in December 1996, TMA officials had not opened the DSO letters, much less used the information to determine whether the individuals had received medical benefits during periods when they were ineligible. TMA officials considered the potential fraud to be against DEERS and, therefore, not requiring their action.

Subsequently, in October 1997, TMA Program Integrity Branch officials advised us they had reviewed all 7,496 letters and determined that none required further action. The officials, however, could not furnish us information on when the reviews had been accomplished, how many of the 7,496 individuals received medical care after becoming ineligible for military benefits, or the dollar amounts (estimated Government losses) involved. They had not entered any data on the individuals in official TMA records. The officials, however, reemphasized their position that they did not need a data system to track potential fraud cases.

In May 1997, working with DMDC officials, we asked TMA to use the CHAMPUS Detail Information System (CDIS) and run a computer match on the individuals identified in the 7,496 letters sent to TMA. The CDIS contains 6 years of medical data on all individuals who have received TRICARE (or prior CHAMPUS) benefits. Between May and December 1997, TMA attempted various computer data matches to satisfy our request. None was completely successful.

DSO Has Implemented a Partial Solution

In mid-1997, the DEERS Support Office initiated a partial solution to the problems involved in reviewing potential ineligibility cases. DEERS Support Office personnel were trained on operating the TRICARE data system and began comparing eligibility dates against TRICARE usage data from MTFs to identify potential ineligibility cases. DSO adopted a \$25,000 loss-to-the-Government threshold for referring such a case to the appropriate MCIO.

The matching process that the DEERS Support Office implemented is a good initial step in addressing potential ineligibility fraud cases. This process, however, is incomplete in that it does not include specific guidance on how DSO, or the TRICARE Management Activity, should process these potential cases. In addition, the \$25,000 threshold for criminal investigative referrals appears to be excessive and not based on cost considerations, such as the cost to investigate and prosecute an ineligibility case. The MCIOs should have various costs and other data that DSO could use in determining whether a specific case should be referred for investigation. Most importantly, the current process does not address how TMA or DSO should pursue possible administrative remedies for:

- ineligibility cases not referred for criminal investigation and prosecution;
- or
- ineligibility cases referred for criminal investigation, but not ultimately prosecuted.

On the contrary, it appears that DSO's referral threshold will result in DoD effectively "forgiving" those cases involving less than \$25,000.²⁵ Such a result would be contrary to existing policy that requires the TRICARE Management Activity to undertake administrative recoupment actions.

Contract Providers and Payment Centers

We also visited three TRICARE contractors and one payment center to review their processes for developing potential TRICARE fraud and abuse cases. As opposed to internal TRICARE procedures, each contractor that we visited had a systematic approach to reviewing, documenting, and referring ineligibility cases. These procedures included referring the case for TMA review and guidance prior to initiating an administrative recoupment action. The referral packages contained complete documentation on patient visits and costs.²⁶

RECOMMENDATION, MANAGEMENT COMMENTS, AND OUR RESPONSE

C. We recommend that the Director, TRICARE Management Activity, with input from the Military Criminal Investigative Organizations, implement a system for developing, referring for criminal investigation, and tracking cases that involve military health care provided to suspected ineligible individuals. This system should include procedures and timelines for pursuing administrative remedies in cases determined not to warrant criminal investigation and prosecution. It should also include procedures and timelines for pursuing administrative remedies in cases referred for criminal investigation, but ultimately not prosecuted, unless a determination is made that the individual was eligible for the health care received.

OUSDP(P&R) nonconcurred, advising that:

²⁵ If applied to actual 1995 through 1997 criminal investigations, this threshold would eliminate 91 percent of the total (see Footnote 32).

²⁶ One contractor that we visited referred 227 potential fraud cases to TMA during the 18 months preceding our visit. Of the total referrals, 25 (11 percent) concerned eligibility. At the time of our visit, however, the contractor had not received any TMA guidance on the 25 eligibility cases.

- the Uniformed Services are responsible for determining eligibility;
- TMA requires DEERS edits to validate each claim processed;
- if DEERS incorrectly indicates eligibility and this is discovered, TMA has procedures and time frames for taking appropriate action, whether or not fraud is suspected; and
- military treatment facilities and dental treatment facilities:
 - have procedures for confiscating invalid ID cards presented by beneficiaries upon being admitted into the facility or for outpatient medical care;
 - perform DEERS checks to determine eligibility and authorize access to care;
 - review ID cards to ensure they have not expired; and
 - have the patient affairs function and hospital security staff work together to confiscate the ID card and further handle the matter with the beneficiary if they determine the beneficiary has lost eligibility or the individual's ID card has expired.

These comments are not responsive to our findings that led to this recommendation. In the draft report, we recognized that ASD(HA) and the Military Departments all have policies requiring medical treatment facilities and TRICARE providers to verify eligibility when an individual requests medical services. In addition, as noted in the report, the locations we visited all had procedures to effect this policy. However, we found that these policies and procedures were not applied consistently and were not fully effective in detecting ineligible individuals. As shown in Table 1, only one of eight (12.5 percent) hospitals and clinics that we visited was performing DEERS checks to ensure eligibility prior to treating walk in/scheduled appointment patients. Further, only two of six hospitals (33.3 percent) were checking DEERS for eligibility prior to admitting patients into the hospitals.

We also found that, even though policy authorizes confiscating identification cards from ineligible individuals, current policies and procedures do not ensure confiscation. As noted in Part II, Section B of this report, only two of eight MTFs (25 percent) that we visited attempted to confiscate identification cards from individuals who could not prove eligibility or who presented an expired identification card. Furthermore, MTF officials recognized that confiscation was not fully effective. As pointed out in the report, in fact, some officials advised us that:

- individuals with invalid identification cards usually leave before security personnel arrived; and
- questionable cardholders seldom reach the patient affairs office “because there are many doors between the administrative desks and ... [the patient affairs office].”

We could not determine the full extent of this problem because the facilities that we visited did not maintain records on the ID cards they questioned or confiscated. However, as discussed in the report, 37 percent of DCIO ineligibility investigations conducted during 1995 through 1997 involved divorced spouses. Fifty percent of these

divorce cases involved divorces that had been final for at least 1 year and the time ranged from 1 year to 26 years. Based on the investigative files, an MTF or TRICARE provider had confiscated the ID card in only 6.7 percent of the divorce cases. Clearly, the current policies and procedures do not ensure that ID cards are confiscated from ineligible cardholders.

Furthermore, we found that TMA does not have a documented system for developing, referring, or tracking potential ineligibility fraud offenses warranting criminal investigation and, as a result, cannot identify the extent to which potential ineligibility cases are referred for investigation. TMA also does not have a documented system and cannot identify the extent to which potential ineligibility cases are referred for administrative action, or the results of either administrative or investigative actions. Overall, we found that this situation exemplifies a condition in which the DoD does not have an effective program to prevent, detect, or investigate ineligibility health care fraud. We believe that ASD(HA) should implement our recommendation to overcome this condition.

Additional OUSD(P&R) comments on this section of the draft report.

1. OUSD(P&R) advised that we incorrectly stated TMA officials had not opened the 7,496 letters from DSO at the time of our visit in December 1996. According to OUSD(P&R), the letters were opened on a daily basis and, where it was determined TRICARE dollars had been spent, referrals were made to the fiscal intermediaries to initiate recoupment. OUSD(P&R) also advised that our evaluator was provided boxes of documents substantiating both the TMA referrals and resulting responses from the fiscal intermediaries confirming initiation of recoupment action.

Our case record does not support the management comments. At the time of our research visit in December 1996, TMA officials had not opened the DSO letters and advised us that they did not plan to do so.²⁷ They related several reasons, including staff limitations, the limited benefits possible from resolving beneficiary fraud cases, and a belief that the potential fraud involved in the DSO letters constituted fraud against DEERS and not warranting their involvement. Subsequently, in October 1997, TMA officials advised us that they had completed reviewing the DSO letters, but could not furnish any supporting records or information. We then learned that, following a meeting held at TMA on April 22-23, 1997, the DSO letters were transferred to DMDC offices in Monterey, California, to be part of a potential “partnership” effort between DMDC, DSO, and Operation Mongoose.²⁸ The potential partners met to determine the best way to

²⁷ Nonetheless, we examined one of the boxes containing the DSO letters, which were located throughout the TMA Program Integrity Branch, and confirmed these letters were unopened.

²⁸ Operation Mongoose is a joint IG, DoD, Defense Finance and Accounting Service (DFAS), and DMDC project that uses computer matching and other techniques to identify potential problems with Government payments to retirees, vendors, “ghost” employees, and transporters/haulers.

review the letters that had been sent to TMA and Operation Mongoose’s potential role in the efforts. As a result of the meeting:

- two DSO employees and one Operation Mongoose employee were trained on using the CDIS; and
- 9,001 DSO letters, including the 7,496 letters originally sent to TMA and additional letters that DSO continued to generate after it stopped referring them to TMA, were transferred to Monterey where DSO and Operation Mongoose could compare individual ineligibility identified in the letter with information in CDIS files.²⁹

We recognize the overall efforts of OUSD(P&R) to address the ineligibility issue that DSO identified. However, such special efforts should not have been necessary. In accordance with OCHAMPUS 5105.2-M, TMA is responsible for planning, developing, and evaluating projects for preventing, detecting, and controlling program fraud, waste, and abuse. TMA is also responsible for conducting specialized investigations when an individual or entity is suspected of program fraud, waste, or abuse. Despite these responsibilities, TMA did not aggressively pursue ineligibility issues when DSO brought those issues to its attention. Furthermore, as discussed in the report, TMA does not have a documented, systematic process for developing, referring, or tracking investigative referrals or administrative actions involving military health care matters. It would appear that TMA must have such a process to meet its responsibilities. As pointed out in the draft report, this situation was part of an overall condition that precluded us from determining, or even reasonably estimating, the extent to which DoD has a problem with ineligibles receiving military health care, or the resulting unauthorized cost that DoD incurs.

2. OUSD(P&R) also clarified information related to TMA and DMDC efforts, at our request, to use the CHAMPUS Detail Information System and run a computer match on the individuals identified in the 7,496 letters. In the draft report, we indicated that the efforts were unsuccessful due to missing TRICARE data. However, OUSD(P&R) advised that:

- they were unaware of any missing information and, in fact, CDIS is accepted in court cases as complete and valid; and
- although the computer runs may not have provided the information the evaluation team desired, TMA is unaware the evaluation team raised a concern about missing information at the time they received the data.

We did not intend to imply a problem with CDIS data completeness or validity. Our reference to missing TRICARE data was intended to refer to our inability to obtain complete “fraud and abuse” case information from TMA, which we discussed at length in

²⁹ At the time of our field visit to DMDC in December 1997, DSO employees were continuing the reviews. However, we doubted complete success due to the age of the cases at that point and because CDIS would not identify all health care an individual may have received after becoming ineligible.

the draft report. However, to avoid confusion, we have amended language in the final report.

3. OUSD(P&R) also provided a correction related to whether TMA or DSO has a \$25,000 threshold for referring potential beneficiary fraud cases for criminal investigation. In the draft report, we recognized that DSO had adopted such a threshold, but observed that TMA apparently intended to forgive beneficiary fraud cases below the threshold. OUSD(P&R) indicated that TMA Program Integrity does not have a dollar limit on the provider or beneficiary fraud cases it accepts. The final report includes the correction.

4. In addition, OUSD(P&R) questioned a statement in the draft report dealing with the amount of fraudulent claims that two contractors we visited had denied. According to OUSD(P&R):

- contractors must forward all fraud cases to the TMA Program Integrity Branch and must also furnish reports that identify fraud and abuse savings; and
- based on the contractor case referrals and reports, in no single 6 month period were dollars reported that come anywhere close to the amounts quoted in the draft report.

OUSD(P&R) is correct. Upon reviewing the factual information, we determined that the total amount referenced in the draft report was not fraudulent claims, but total claims processed, and that the amount identified as ineligibility fraud was the total denial amount. Since this statement was not central to the overall discussion, we have deleted it from the final report.

D. MOST CRIMINAL INVESTIGATIONS INVOLVING INELIGIBILITY ARE CLOSED WITHOUT CRIMINAL, CIVIL, OR ADMINISTRATIVE REMEDY, AND THE REMAINDER DO NOT RECOVER ESTIMATED GOVERNMENT LOSSES

Most (66 percent) criminal investigations involving ineligibility that were conducted during 1995 through 1997 were not accepted for prosecution, or were closed without criminal, civil, or administrative remedies. Further, those investigations that did result in criminal, civil, or administrative remedies produced monetary recoveries equal to only 5.1 percent of the estimated Government losses. Based on these investigative outcomes, unless OASD(HA) requires aggressive administrative recoupment actions, most unauthorized costs that DoD incurs from ineligibility medical fraud will not be recovered.

Introduction

The IG, DoD “Revised Interim Guidance for Criminal Investigations of Fraud Offenses Jurisdiction,” October 23, 1996, assigns the MCIOs primary responsibility for investigating military health care fraud committed by beneficiaries. We met with representatives from each MCIO headquarters and 12 field offices to review their procedures and processes for investigating potential ineligibility fraud cases and referring them for prosecution or administrative actions. We also asked the DCIOs for data on their 1995, 1996, and 1997 criminal investigations that involved alleged ineligibility fraud.

DCIO Investigations Involving Ineligibility for Medical Care

During calendar years 1995 through 1997, the DCIOs continued 4 investigations opened prior to 1995, opened 77 new investigations (81 total investigations), and closed 74 investigative cases that involved potential ineligibility for medical care.³⁰ The 81 total investigations³¹ involved a total \$1.4 million estimated Government loss for military

³⁰ Three of these cases involved investigative activity, but never became full investigations because initial investigator contacts with prosecutors disclosed they did not have prosecution appeal.

³¹ Seventeen of these cases were included in the TMA case listings (22 total cases) discussed previously. However, there is no evidence that they were investigative case referrals from any OASD(HA) organization. Further, while medical personnel were sources of the allegations causing some of the criminal investigations, most (53, or 65 percent) resulted from allegations from other sources. Based on the records maintained, we could not determine if any actual criminal investigation addressed an ineligibility issue identified in the 7,496 letters that the DEERS Support Office sent to the TRICARE Management Activity.

medical care given to allegedly ineligible individuals.³² Of the 74 closed investigations, 25 (34 percent) were closed with one or more types of remedial results, including criminal prosecutions, civil recoveries, administrative recoveries, or other administrative actions.³³ The remaining 49 cases (66 percent) did not result in prosecutions or other remedial actions. Generally, the latter closures were based on prosecutor decisions that the cases lacked criminal intent, or the amounts involved were too small to warrant prosecutions. Appendix D includes these and other statistics on the DCIO investigations.

Database Checks That Could Assist Investigations

An ineligible individual who obtains an identification card may obtain military health care improperly. Additionally, a sponsor who does not remove a divorced spouse or other ineligible dependent from DEERS may also not remove the ineligible dependent from military pay and housing records, which could result in additional unauthorized costs to the Government. Therefore, including database checks in the criminal investigation could result in identifying other criminal activity by, or improper payments to, an ineligible individual. In any event, the data checks would enhance investigative thoroughness and prosecution potential.

We developed a database checklist for use in reviewing actual MCIO eligibility investigations. Our checklist included the DEERS and TRICARE databases; the local, nearby, or point of residence MTF (i.e., the MTF that most likely would serve the individual receiving medical care); and the local housing office (if an active-duty sponsor). Table 2 below shows the results of comparing our checklist with actual data checks in the 81 ineligibility cases that the DCIOs investigated during 1995 through 1997.

Table 2

Database Checks Conducted During Criminal Investigations

Type of Check	Was the Database Checked?							
	Yes		No		N/A *		Total	
	No.	%	No.	%	No.	%	No.	%
DEERS	36	44	43	53	2	2	81	100

³² The estimated Government loss averaged \$16,765 per case. Forty percent of the cases involved less than \$1,000. Seventy-eight percent involved less than \$10,000. Ninety-one percent involved less than \$25,000.

³³ Only 12 of these cases (16 percent) resulted in monetary recoveries. These recoveries totaled \$39,363, or 5.1 percent of the total estimated loss for the closed cases.

MTF	43	53	36	44	2	2	81	100
TRICARE	30	37	49	60	2	2	81	100
Housing	11	14	8	10	62	76	81	100

- * Includes two cases that we could not determine if database checks would have been applicable. In addition, 60 of the investigations did not involve active-duty members and, accordingly, housing checks were not applicable to these investigations.

As Table 2 shows, data checks were frequently not completed when they were potentially applicable to the cases under investigation:

- DEERS checks were not completed in 53 percent of the cases;
- MTF checks were not completed in 44 percent of the cases;
- TRICARE checks were not completed in 60 percent of the cases; and
- Housing checks were not completed in 10 percent of the cases.

One USACIDC investigation that we reviewed illustrates how conducting these data checks might have identified a higher potential Government loss, thus improving chances for criminal prosecution. This USACIDC investigation involved a spouse who lost eligibility upon divorcing the military sponsor. After becoming ineligible for military health care, the spouse continued to seek emergency treatment personally and for two children. In this case, the investigator checked the DEERS database to confirm ineligibility. The investigator also identified medical costs totaling \$847 for treatments at the local military hospital. Due to the minimal loss to the Government, the Assistant United States Attorney (AUSA) declined the case for prosecution. Had TRICARE records been checked, however, the investigator would have discovered that the individual had received TRICARE benefits totaling over \$33,000 during the overall period after becoming ineligible. The total amount would have exceeded the AUSA's threshold for prosecution. In addition, the investigative file does not indicate that the investigator considered including the sponsor in the investigation even though the sponsor had not reported the status change (divorce) to DEERS as required.

MCIO Access to Databases

An investigator should access specialized databases with information relevant to the investigation. In ineligibility cases, both DEERS and CDIS are specialized databases with highly relevant information. DEERS contains eligibility dates and reasons for eligibility terminations. CDIS contains a 6-year history that covers medical claims from, and payments to, an individual. To receive CDIS data, however, the MCIOs must write to TMA requesting the access, detailing the exact information required, and justifying the need. Following this process to receive CDIS information could significantly delay the criminal investigations.

TMA officials stated concern about allowing the MCIOs ready access to CDIS. They indicated that the system was complicated to use and contained privacy information. However, TMA had granted CDIS access to over 900 users, including DCIS agents, and had trained these system users. The MCIOs should also be given access to, and training on using, CDIS to aid their military health care investigations.

RECOMMENDATIONS, MANAGEMENT COMMENTS, AND EVALUATION RESPONSE

D.1. We recommend that the Director, TRICARE Management Activity, arrange for the Military Criminal Investigative Organizations to receive access to, and system training on using, the CHAMPUS Detail Information System to aid their military health care investigations.

OUSD(P&R) nonconcurrent. According to OUSD(P&R):

- TRICARE has a Memorandum of Understanding with DCIS under which fraud cases are forwarded for investigation;
- DCIS is the lead DoD agency responsible for fraud involving the TRICARE program and includes the MCIOs in health care task forces in those areas where the MCIOs may have jurisdiction;
- experts in Operation Mongoose have access to multiple databases and should be included as a point of contact for the MCIOs to ensure maximum recovery of Government dollars; and
- it is essential that the MCIOs work cooperatively as part of the existing multidisciplinary team to combat health care and other eligibility fraud.

The draft report referenced the MOU between OASD(HA) and DCIS. This MOU was dated June 28, 1995, and initially did provide that TMA would refer to DCIS any potential criminal case involving \$10,000 or more. However, after the MOU was executed, the IG, DoD issued the “Revised Interim Guidance for Criminal Investigations of Fraud Offenses Jurisdiction,” October 23, 1996, assigning the MCIOs primary responsibility for investigating military health care fraud committed by beneficiaries. Following this new guidance, on April 17, 1997, DCIS forwarded a memorandum to TMA advising:

“Paragraph 3.f. of the revised Interim Guidance for Criminal Investigations of Fraud Offenses dated October 23, 1996, states that the ... MCIOs ... have primary jurisdictional responsibility for allegations of fraud perpetrated against ... OCHAMPUS ..., a fiscal intermediary or other health care providers or insurers by Military Service members, military retirees and dependents who

have received, made claims for or requested benefits or services under such program or operation. Accordingly, ... DCIS ... requests that OCHAMPUS refer all allegations of beneficiary fraud to the appropriate MCIO for investigation, regardless of alleged dollar loss to the Government. The DCIS offices have also been advised that such allegations should be referred to the MCIOs...”

Accordingly, while OUSD(P&R) is correct that DCIS is the DoD agency with lead responsibility for investigating fraud involving the TRICARE program, jurisdictional responsibility for beneficiary fraud cases was specifically assigned to the MCIOs. The MCIO investigations would be enhanced with the database access and training that we recommended. They would also be enhanced with the Operation Mongoose contacts that OUSD(P&R) suggested. We have therefore modified our recommendation below to the MCIOs.

D.2. We recommend that the Military Criminal Investigative Organizations implement procedures that ensure their criminal investigators who conduct military health care investigations check all relevant databases, including those under Operation Mongoose cognizance, in determining the types of criminal conduct involved and the resulting total losses to the Department of Defense.

Appendix A. Statutory and Regulatory Authority

Various statutes and regulatory guidance cover eligibility for receiving military benefits and the penalties for misusing or abusing those benefits. The key documents are:

- **Title 10, United States Code, Section 1071 (10 U.S.C. §1071).** Provides for an improved, uniform medical and dental care program for members and certain former members of the Uniformed Services and their dependents.
- **10 U.S.C. §801, et seq. Uniform Code of Military Justice.** Sets out the jurisdiction and procedures for administering discipline in the Armed Forces through judicial and non-judicial proceedings, including courts-martial. Also sets out the specific crimes that may be prosecuted under the Code and the punishments authorized.
- **18 U.S.C. §287 and §1001.** U.S. Criminal Code provisions that address “False, Fictitious, or Fraudulent Claims” and “Fraud and False Statements,” respectively. These provisions are cited on DD Form 1172 as crimes applicable to sponsors who enroll ineligible individuals in DEERS, and ineligible individuals who fraudulently receive military benefits.³⁴
- **Title 32, Code of Federal Regulations, Part 199 (32 C.F.R. §199).** Specifies eligibility for TRICARE and requirements for submitting TRICARE claims.
- **Public Law (P.L.) 104-191, “The Health Insurance Portability and Accountability Act of 1996.”** This Act, commonly known as the Kennedy-Kassebaum Act, establishes health care fraud as a specific crime and facilitates law enforcement (criminal, civil and administrative) in health care matters.
- **Department of Defense Directive (DoDD) 1000.22, “Uniformed Services Identification (ID) Cards,” October 8, 1997.** Establishes DoD policy for issuing ID cards to members of the Uniformed Services, their eligible dependents and other eligible individuals. Assigns USD(P&R) responsibility for the eligibility and enrollment program.
- **DoD Instruction (DoDI) 1000.13, “Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,” December 5, 1997.** Implements DoD policy, responsibilities and procedures for issuing ID cards and establishing eligibility for military benefits and privileges.
- **DoDD 1341.1, “Defense Enrollment Eligibility Reporting System,” October 14, 1981.** Sets forth implementing guidance and procedures for DEERS.

³⁴ Various other criminal provisions could also apply to this type crime, depending on the specific facts and circumstances involved in the criminal action or activity. We are not listing all possible citations to criminal code that might be applicable to an individual case.

- **DoDI 1341.2, “DEERS Procedures,” March 2, 1982.** Delineates DEERS procedures and outlines responsibilities for the DEERS Program Office and Program Manager.

- **IG, DoD, Revised Interim Guidance, “Revised Interim Guidance for Criminal Investigations of Fraud Offenses Jurisdiction,” October 23, 1996.**

Superseded IG, DoD Interim Guidance, “Jurisdiction for Fraud Investigations, June 9, 1995. The interim guidance and revised interim guidance both assigned the MCIOs responsibility for investigating fraud allegations that involve:

- military activities, installations, or facilities, especially those affecting the health, welfare, and morale of military service personnel (or their dependents); and
- OCHAMPUS, a fiscal intermediary, or other health care provider or insurer of military service members, military retirees and dependents who have received, made claims for, or requested benefits or services under such program or operations;

- **Joint Service and Uniformed Services Instruction, “Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel,” March 1, 1998 (the Joint Instruction).** Implements DoD policy for preparing, issuing, using, accounting for, and disposing of military ID cards. Incorporates most Uniformed Services procedures and reflects unique Service information. Issued by order of the various departmental Secretaries, with individual citations as follows:

- Army Regulation 600-8-14;
- BUPERS Instruction 1750.10A, Change 1;
- Marine Corps Order P5512.1B, Change 1;
- Commandant Instruction M5512.1;
- Air Force Instruction 36-3026(I); and
- Commissioned Corps Personnel Manual 29.2, Instructions 1 and 2.

Appendix B. Relevant Prior Reports and Findings

- **GAO-B-133142, “Potential for Improvements in the Civilian Health and Medical Program of the Uniformed Services,” July 19, 1971.** GAO found that the Government was incurring unnecessary CHAMPUS costs because identification cards, showing eligibility, were not being recovered from dependents when military members either separated from or deserted the Service.

- **DAS 79-002, “Report on the Review of Procedures Used to Determine Eligibility of Users of the Uniformed Services Medical Facilities,” October 11, 1978, and DAS 79-014, “Report on the Review of Eligibility of Recipients of Benefits Under the Civilian Health and Medical Program of the Uniformed Services,” November 17, 1978.** The former Defense Audit Service (DAS)³⁵ found that it was not possible to verify whether only eligible persons were given medical services at either Uniformed Service or CHAMPUS medical facilities. Based on these two reports, in 1979, DoD estimated that up to \$60 million annually (\$20 million in direct medical facility costs and \$40 million in CHAMPUS costs) were misspent on ineligible recipients.

- **GAO/HRD-79-58, “Letter Report to the Secretary of Defense,” March 16, 1979.** GAO found that improper CHAMPUS payments were continuing because DoD did not have an eligibility verification system and because controls over issuing and recovering identification cards were weak. Procedures were inadequate for recovering identification cards from divorced spouses and from dependents of active duty members who separated early from military service. According to GAO, one type of potentially erroneous CHAMPUS payment (for health care provided to dependents after the sponsors separated from active duty) cost the Government an estimated \$780,000 over a 26 month period.

- **GAO/HRD-83-1, “Verifying Eligibility for Military Health Care: Some Progress Has Been Made, But Reliability Problems Remain,” December 1, 1982.** GAO found that MTFs were performing only about 13 percent of required DEERS checks, thus potentially allowing ineligible individuals to receive medical care. GAO also found that DoD was not taking actions to resolve potential problems when discrepancies were identified in DEERS information. In addition, GAO found that sponsors were not reporting changes in dependent status, especially divorces.

- **OIG, DoD INS-PED-015, “Review of Health Care Fraud Detection and Prevention within the Department of Defense,” February 24, 1994.** The then Office of Assistant Inspector General for Inspections, OIG, DoD, compared DoD health care fraud detection and prevention techniques against private sector techniques. The

³⁵ DAS was incorporated into the OIG, DoD, as the Office of the Assistant Inspector General for Auditing, when the OIG, DoD, was established.

OIG, DoD, determined that DoD had not developed an anti-fraud strategy, and was not providing health care fraud training or networking opportunities for its investigators.

- In November 1996, the then Office of Assistant Inspector General for Policy and Oversight, OIG, DoD, announced an “Evaluation of Health Care Beneficiary Fraud Investigations.” During the research phase of the project, the OIG, DoD, determined that a Memorandum of Understanding (MOU) between OASD(HA) and DCIS, the OIG, DoD criminal investigative arm, was in conflict with the jurisdictional responsibilities outlined in the “Revised Interim Guidance for Criminal Investigation of Fraud Offenses Jurisdiction,” October 23, 1996. The revised interim guidance assigned responsibility for beneficiary fraud investigations to the MCIOs. The MOU, however, required the CHAMPUS Support Office (now DSO) to refer all beneficiary cases involving \$10,000 or more, or involving flagrant issues, to DCIS. On April 17, 1997, DCIS effectively modified this MOU by notifying TMA and the DCIS field offices that all beneficiary fraud cases, regardless of alleged dollar loss, should be referred to the appropriate MCIO. On March 13, 1997, based on several factors, including DCIS advice that it was modifying the MOU, the OIG, DoD, canceled the planned evaluation.

Appendix C. Sites Visited During the Evaluation

MILITARY INSTALLATIONS

Army

- Fort Belvoir, VA
- Fort Lewis, WA
- Fort Sam Houston, San Antonio, TX

Navy and Marine Corps

- Naval Air Station, Patuxent River, MD
- U.S. Navy Personnel Support Activity, San Diego, CA
- U.S. Marine Corps Camp Pendleton, San Diego, CA

Air Force

- Kelly AFB, San Antonio, TX
- Lackland AFB, San Antonio, TX
- Randolph AFB, San Antonio, TX
- Tinker AFB, Oklahoma City, OK
- Vance AFB, Enid, OK

Joint Service

- Carswell Joint Reserve Training Base, Fort Worth, TX

MEDICAL TREATMENT FACILITIES

Army

- Brooke Army Medical Center, Fort Sam Houston, TX
- Madigan Army Medical Center, Fort Lewis, WA

Navy

- Balboa Naval Hospital, San Diego, CA
- Naval Hospital, Camp Pendleton, CA
- Naval Medical Clinic, Patuxent River, MD

Air Force

- Tinker Air Force Base Hospital, Oklahoma City, OK
- Vance AFB Clinic, Enid, OK
- Wilford Hall Medical Center, Lackland AFB, TX

TRICARE CONTRACTORS AND PAYMENT CENTERS

- Foundation Health, Surfside Beach, SC
- Foundation Health Services, Rancho Cordova, CA
- Humana, Louisville, KY
- Tri-West Healthcare Alliance, Phoenix, AZ
- Blue Cross/Blue Shield Payment Center, Myrtle Beach, SC
- TRICARE Payment Center, Myrtle Beach, SC

Appendix D. Criminal Investigations Conducted 1995 – 1997 (Ineligibility Cases)

NO.	CASE NUMBER	SUBJ. NO.	DATE OPENED	DATE CLOSED *	SOURCE OF ALLEGATION	ESTIMATED LOSS	REMEDIAL RESULTS					
							NONE **	\$\$ ***	Confinement ****	Article 15	Discharge	Admin Action
Closed Cases												
1	0013-96-CID142-32112	1	01/23/1996	08/13/1997	Anonymous Tip	\$24,419						X
	0013-96-CID142-32112	2	01/23/1996	08/13/1997								
2	0034-97-CID045-68713	1	02/08/1997	04/25/1997	Other Agency	\$1,600						
	0034-97-CID045-68713	2	02/08/1997	04/25/1997								X
3	0043-96-CID062-31819	1	06/06/1996	07/22/1996	Command	\$11,219		11,219				
4	0043-96-CID637-20713	1	02/09/1996	04/17/1996	Other Agency	\$978					X	
5	0058-97-CID032-57713	1	01/29/1997	03/31/1997	MTF	\$4,183	2					
6	0074-95-CID043-49109	1	02/25/1995	07/12/1995	Source Information	\$3,293	1					
7	0077-96-CID022-30267	1	03/14/1996	06/21/1996	Source Information	\$1,509	2					
8	0079-95-CID013-51326	1	02/09/1995	03/15/1995	MTF	\$1,024	1					
9	0094-96-CID446-44007	1	03/20/1996	11/08/1996	IG	\$2,988	1					
	0094-96-CID446-44007	2	03/20/1996	11/08/1996								
10	0102-96-CID083-37308	1	04/04/1996	06/07/1996	Source Information	\$4,468	1					X
11	0114-97-CID083-62364	1	03/20/1997	09/24/1997	Source Information	\$672	1					
	0114-97-CID083-62364	2	03/20/1997	09/24/1997								
12	0116-95-CID073-53021	1	05/02/1995	08/17/1995	Other Agency	\$1,631	1					
13	0138-95-CID073-53822	1	06/07/1995	10/16/1995	From Other Agency	\$29,953						
	0138-95-CID073-53822	2	06/07/1996	10/16/1996			1					
14	0164-96-CID056-43616	1	03/07/1996	04/16/1996	Source Information	\$2,998	2					
15	0171-96-CID014-43291	1	03/26/1996	06/10/1996	USACIDC	\$10,423	1					
16	01APR97-NFNF-0400-4UCR	1	04/01/97	4/2/97	Source Information	\$0	2					
17	01FEB94-05LE-0080-4UMA	1	02/01/94	2/9/95	Command	\$61					X	
	01FEB94-05LE-0080-4UMA	2	02/01/94	2/9/95								
	01FEB94-05LE-0080-4UMA	3	02/01/94	2/9/95								
	01FEB94-05LE-0080-4UMA	4	02/01/94	2/9/95								
18	01FEB96-MWDT-0004-4UCR	1	02/01/96	2/15/96	TRICARE	\$0						
19	0207-96-CID056-43628	1	03/27/1996	04/16/1996	Source Information	\$2,218		2,218	X			
20	0237-96-CID083-37336	1	08/09/1996	08/21/1996	Proactive	\$1,015						X
21	0254-96-CID013-35957	1	05/10/1996	06/11/1996	Source Information	\$568	1	568				
22	0259-95-CID145-20829	1	12/04/1995	12/15/1995	OCHAMPUS	\$38,136	1					

Appendix D. Criminal Investigations Conducted 1995-1997 (Ineligibility Cases)

23	0260-96-CID053-35433	1	07/25/1996	02/14/1997	Other Agency	\$1,786	2					
	0260-96-CID053-35433	2	07/25/1997	02/14/1997								
24	0260-97-CID073	1	10/15/97	10/16/97	CHAMPUS	\$34,037	1					
	0260-97-CID073	2	10/15/97	10/16/97								
25	0284-96-CID083-37344	1	09/24/1996	11/06/1996	USACIDC	\$591	1					
26	02APR96-NFHV-0030-4UNA	1	04/02/96	9/25/96	MTF	\$2,500	2					
27	02JAN96-NFNF-0002-4UNI	1	01/02/96	5/20/96	Proactive	\$0	2					
28	0323-95-CID054-22674	1	06/20/1995	7/21/1995	MTF	\$847	1					
29	0325-97-CID043-64787	1	08/18/1997	09/05/1997	Source Information	\$569	1	569				
	0325-97-CID043-64787	2	08/18/1997	09/05/1997								
30	0336-97-CID093-61642	1	07/22/1997	08/26/1997	Source Information		2					
31	0362-95-CID137-33404	1	11/16/1995	10/21/1996	Anonymous Tip	\$192		300			X	
	0362-95-CID137-33404	2	11/16/1995	10/21/1997								X
32	0366-97-CID056-69917	1	05/01/1997	05/09/1997	Other Agency	\$759					X	
	0366-97-CID056-69917	2	05/01/1997	05/09/1997							X	
	0366-97-CID056-69917	3	05/01/1997					759				
33	0377-95-CID024-20101	1	07/17/1995	09/19/1995	USACIDC		2					
34	0424-95-CID054	1	8/23/1995	09/07/1995	Source Information	\$18,900	2					
35	0438-96-CID044-42421	1	10/23/1996	03/03/1997	Other Agency	\$9,550				X		
	0438-96-CID044-42421	2	10/23/1996	03/03/1997								
36	0441-94-CID043-31398	1	01/19/1995	01/19/1995	Source Information	\$891						X
37	04AUG97-CAP1-0103-4UNA	1	08/04/97	12/19/97	Command	\$1,382		1,382				
38	0500-97-CID044-67869	1	12/02/1997	12/31/1997	Command	\$9,614	2					
39	0550-96-CID013	1	10/1/96	10/10/96	Proactive		2					
40	0571-95-CID034-21527	1	07/07/1995	12/30/1995	Other Agency		2					
41	0602-96-CID016-44855	1	07/31/1996	10/01/1996	Source Information	\$808		808				
42	08DEC95-MPJX-0042-4UNA	1	12/08/95	3/24/97	Source Information	\$0	2					
43	08MAY97-CACP-0067-4UMA	1	05/08/97	5/20/97	MTF	\$0	2					
44	12OCT93-11SD-1427-4UNA	1	10/12/93	2/24/95	Command	\$17,007			X		X	
	12OCT93-11SD-1427-4UNA	2	10/12/93	2/24/95								X
45	13JUL95-NFHV-0043-4UNA	1	07/13/95	8/29/95	MTF	\$385	1					
46	13MAR96-NFCE-0060-4UNA	1	03/13/96	5/23/96	Command	\$0	2					
	13MAR96-NFCE-0060-4UNA	2	03/13/96	5/23/96								
47	13SEP93-20WA-4009-4UNA	1	09/13/93	4/12/95	Source Information	\$2,417		2,417				
	13SEP93-20WA-4009-4UNA	2	09/13/93	4/12/95								
48	14MAR95-GCCC-0071-4UNA	1	03/14/95	3/20/95	Other Agency	\$6,292	2					
49	16OCT95-GCNR-0009-4UNA	1	10/16/95	6/19/97	Referred by DCIS	\$13,428	2					
50	23MAR95-CSKB-0139-4UNA	1	03/23/95	7/28/95	Other Agency	\$0	2					
51	25JAN95-GCPC-0017-4UNA	1	01/25/95	2/1/96	Source Information	\$3,836	1					
52	28JUL94-05NF-1280-4UNA	1	07/28/94	1/10/95	Source Information	\$0	2					
53	28MAR95-NFNF-0820-4UNI	1	03/28/95	1/16/97	Anonymous Tip	\$5,483	1					

Appendix D. Criminal Investigations Conducted 1995-1997 (Ineligibility Cases)

54	30MAR95-NFNF-0846-4UNI	1	03/30/95	6/20/96	Referred by DCIS	\$0	2					
55	9511209C	1	06/12/95	8/97	TRICARE	\$362,941	1					
	9511209C	2	06/12/95	8/97								
	9511209C	3	06/12/95	8/97								
56	9511231Y	1	06/19/95	6/95	TRICARE	\$11,206	2					
57	95211D4-S762954	1	02/02/95	7/7/95	Medical Personnel	\$2,908		2,908				X
58	95219D61-S765366	1	03/15/95	5/3/95	Medical Personnel	\$0	2					
59	95323D58-S715691	1	10/02/95	11/14/95	None	\$0	2					
60	9610089C	1	10/27/95	10/95	TRICARE	\$6,711	2					
61	9610159Z	1	11/30/95	9/96	TRICARE	\$11,624	1					
	9610159Z	2	11/30/95	9/96								
62	96206D4-S796832	1	08/22/96	8/15/97	Medical Personnel	\$5,103		5,103				
63	96206D4-S796833	1	08/22/96	8/15/97	Medical Personnel	\$6,272						X
64	96211D4-S801457	1	11/13/96	3/26/97	Medical Personnel	\$45,646			X	X		X
	96211D4-S801457	2	11/13/96	3/26/97								
65	96216D4-S786881	1	02/20/96	4/2/96	SJA	\$0					X	
66	96216D4-S786948	1	02/21/96	4/2/96	SJA	\$1,682	2					
67	96301D4-S797065	1	08/27/96	1/10/97	Medical Personnel	\$11,112		11,112				
68	96303D61-S786700	1	02/15/96	8/26/96	Medical Personnel	\$1,603						X
69	96303D61-S795950	1	08/05/96	1/10/97	Open Source-Civilian	\$4,846	1					
70	96320D95-S790713	1	04/20/96	7/20/96	None Entered	\$0						X
71	9710017S	1	10/09/96	3/97	TRICARE	\$7,932	1					
72	9710051A	1	10/23/96	6/97	TRICARE	\$0	2					
	9710051A	2	10/23/96	6/97								
73	9710231I	1	01/13/97	10/97	TRICARE	\$11,429	2					
74	97211D4-S807219	1	03/04/97	5/8/97	Open Source-Military	\$12,193						X
	97211D4-S807219	2	03/04/97	5/8/97								
74	Subtotal - Closed Cases	98				\$777,838	49	\$39,363	3	2	7	13
	Average Per Case	1.3				\$10,511		\$532				
91%	Percent of Cases						66%		4%	3%	9%	18%
Open Cases												
1	0362-97-CID022-59100	1	10/03/1997		MTF	\$474	1	474				
2	06OCT97-FEYK-0331-4UNI	1	10/06/97		MTF	\$65,000						
3	08MAY96-MPIX-0109-4UNA	1	05/08/96		TRICARE	\$91						
4	9610390G	1	02/20/96		Other Agency	\$500,000						
5	9610517N	1	04/08/96		TRICARE	\$4,043						
6	9710253E	1	01/22/97		TRICARE	\$9,408	1					X
7	0239-97-CID967-53866	1	09/10/1997		Command	\$1,093		1,093		X		
	0239-97-CID967-53866	2	09/10/1997				1					

Appendix D. Criminal Investigations Conducted 1995-1997 (Ineligibility Cases)

7	Subtotal – Open Cases	8				\$580,109	3	\$1,567	0	1	0	1
	Average Per Case	1.1				\$82,873		\$224				
9%	Percent of Cases						43%		0%	14%	0%	14%
81	Total Cases	106				\$1,357,947	52	\$40,930	3	3	7	14
	Average Per Case	1.3				\$16,765		\$505				
100%	Percent of Cases						64%		4%	4%	9%	17%

* ROI date where the case closure date was not provided.

** 1 = Prosecution Declined; 2 = Prosecution Was Not Declined, But Case Was Closed Without Criminal, Civil, or Administrative Remedy

*** Total monetary recoveries, including fines, penalties, restitutions and recoveries.

**** Includes suspended sentence time and probation time.

Appendix E. Management Comments



PERSONNEL AND
READINESS

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000



100-100-1

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL (CRIMINAL
INVESTIGATIVE POLICY AND OVERSIGHT)

SUBJECT: Response to Draft Report on the Evaluation of the Investigative Environment in
Which the Defense Enrollment Eligibility Reporting System Operates (Project
No. 70F-9029)

Thank you for the opportunity to review and comment on the draft report evaluating whether the Department of Defense (DoD) is effective in preventing, detecting, and investigating instances in which ineligible individuals obtain identification cards, and the benefits they receive from using these cards.

Recommendation A. The Under Secretary of Defense (Personnel and Readiness), through the Joint Uniformed Services Personnel Advisory Committee, establish time limits for sponsors to (1) report a change in eligibility status for their dependents, and (2) surrender a dependent's identification card when the dependent becomes ineligible for military benefits and privileges, and adopt these time limits in appropriate policy.

Response: Concur. The Joint Uniformed Services Personnel Advisory Committee has been asked to establish time limits.

Recommendation B. The ASD(HA) direct medical treatment facility commanders to comply with existing policy that requires 100 percent eligibility checks, confiscating identification cards, and initiating recoupment actions for costs incurred.

Response: Concur. We plan to complete our implementation by November 1, 1999.

Recommendation C. The ASD(HA) should (1) require the TRICARE Management Activity to implement an aggressive management control plan with fraud indicators that helps detect ineligible individuals who apply for and receive medical care through TRICARE, and (2) consider making this plan part of the TRICARE Management Activity's Annual Statement of Assurance submitted in accordance with DoD Directive 5010.38, "Management Control Program," August 26, 1999.



Response: Nonconcur. The determination of a person's eligibility as a TRICARE/CHAMPUS beneficiary is the responsibility of the Uniformed Services. TRICARE does not have the authority to determine eligibility or to terminate it (see 32 C.F.R.199.3 and DoDI 1000.13). Therefore, a management control program more properly lies with the Uniformed Services to ensure that the information in DEERS is accurate and valid. TMA does have the authority for mandating that DEERS be accessed for each claim to ensure the individual is eligible for the dates of service being billed. This is currently being done. In addition, as indicated above, MTFs will perform a 100% DEERS eligibility check for care done in the direct care system. The existence and use of an accurate centralized eligibility database is a major fraud control tool.

Recommendation D: The Executive Director, TRICARE Management Activity, with input from the Military Criminal Investigative Organizations (MCIOs), implement a system for developing, referring, and tracking cases that involve military health care given to suspected ineligible recipients. This system should include procedures and timelines for pursuing administrative remedies in cases determined not to warrant criminal investigation and prosecution. It should also include procedures and timelines for pursuing administrative remedies in cases referred for criminal investigation, but ultimately not prosecuted, unless a determination is made that the individual was eligible for the medical treatment received.

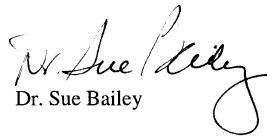
Response: Nonconcur. As indicated above the Uniformed Services are responsible for determining eligibility. TMA requires that each claim processed be validated by the DEERS edit. If DEERS incorrectly indicates eligibility and that is discovered, TMA already has in place procedures and time frames for taking appropriate action, whether or not fraud is suspected.

Additionally procedures exist at military treatment facilities/dental treatment facilities to confiscate invalid ID cards that are presented by beneficiaries upon their being admitted into the facility or for outpatient medical care. In order to determine eligibility and authorize access to care, the medical facility performs a DEERS check. Additionally, ID cards are reviewed to ensure they have not expired. If it is determined that either the beneficiary has lost eligibility or the ID card has expired, the patient affairs function of the medical facility is notified who in turn works with the hospital security staff to confiscate the ID card and further handle the matter with the beneficiary.

Recommendation E. The Executive Director, TRICARE Management Activity, arrange for the MCIOs to receive access to and system training on the CHAMPUS Detail Information System (CDIS) to aid their military health care investigations. The MCIOs should implement procedures to ensure their criminal investigators who conduct military health care investigations check all relevant databases in determining the types of criminal conduct involved and the resulting overall losses to the Department of Defense.

Response: Nonconcur. TRICARE has a Memorandum of Understanding with the DoD-IG Defense Criminal Investigative Service (DCIS) under which cases of TRICARE fraud are forwarded for investigation. DCIS is the lead DoD agency responsible for fraud involving the TRICARE program. DCIS includes the MCIOs in health care task forces in those areas where the MCIOs may have jurisdiction. Operation Mongoose is an example of an approach involving eligibility issues within the DoD. The experts in Operation Mongoose have access to multiple databases and should be included as a point of contact for the MCIOs to ensure maximum recovery of government dollars. It is essential that MCIOs work cooperatively as part of the existing multidisciplinary team to combat health care and other eligibility fraud.

In addition to the above responses to the recommendations, we have also attached a separate statement of our concerns as to the accuracy and completeness of some sections of the report. We would be happy to further discuss these with you at your convenience. Our point of contact is Ms. Rose Sabo, Chief, Program Integrity, TRICARE Management Activity, Aurora, Colorado. She may be reached at (303) 676-3478.


Dr. Sue Bailey

Attachment:
As stated

Statement of Concerns as to the Accuracy and Completeness of Some Sections of Draft Report on "Evaluation of the Criminal Investigative Environment In Which the Defense Enrollment Eligibility Reporting System Operates"

The statement (page 25) that "TMA officials in both program integrity and legal" directly limited actions on beneficiary fraud are inappropriate and taken out of context. Those comments concerned the referrals that the author apparently believed were fraud cases, when in fact they represented no fraud but erroneous issuance of ID cards involving individuals who had lost eligibility for CHAMPUS/TRICARE because they had attained eligibility for Medicare Part A, under age 65, due to disability or end stage renal disease. In these cases, ID cards were issued by Uniformed Service personnel in the mistaken belief that the beneficiary was eligible for CHAMPUS/TRICARE. The cases were not entered into the fraud tracking system simply because they did not involve fraud. Because these patients were unaware that they had lost eligibility for CHAMPUS/TRICARE, they continued to use CHAMPUS/TRICARE benefits.

When it was determined that the patients were not eligible for CHAMPUS/TRICARE, the Federal Claims Collection Act required the agency to take aggressive collection action to pursue recoupment of the erroneous payments that were made to patients and to their providers. Once collection action was initiated against a provider, the providers frequently pursued collection from the patient who received the services. As a result, thousands of disabled and very ill individuals were forced to deal with a myriad of collection actions including forceful demand letters, harassment by collection agencies, lawsuits and adverse credit ratings. One patient died of a heart attack while awaiting a meeting with his Congressman (the then Speaker of the House) concerning the recoupment action. His family attributed his death to stress caused by the aggressive collection action taken against him. In another case, the Surgeon General of the Air Force interceded on behalf of a patient incapacitated by amyotrophic lateral sclerosis (Lou Gehrig's syndrome), who was also receiving demands for payment.

Once Congress became aware of the hardship imposed by these collection actions, it passed legislation authorizing waiver of collection of payments, retroactive to January 1, 1967. See Section 743 of PL 104-106. Because eligibility for CHAMPUS/TRICARE is restored once an individual obtains coverage under Medicare Part B, Congress also passed legislation extending CHAMPUS/TRICARE eligibility for these individuals through July 1, 1999 to give them the opportunity to enroll in Medicare Part B and retain their benefits. See Section 704 of Public Law 105-261. It would have been highly irresponsible to pursue these cases as involving potential fraud when it was clear that the vast majority of them resulted by classification error on the part of the Government.

The statement (page 29) that TMA officials had not opened the 7,496 letters from DSO at the time of the DoD IG visit in December 1996 is incorrect. The letters were opened on a daily basis and, where it was determined TRICARE dollars had been spent, referrals were made to the fiscal intermediaries to initiate recoupment. The evaluator was provided boxes of documents substantiating both TMA's referrals and the resulting responses from the fiscal intermediaries confirming initiation of recoupment action.

Attachment

As to the assertion of missing TRICARE data on the CDIS (page 30), we are not aware of any missing information. In fact, CDIS is accepted in court cases as complete and valid. Although the computer runs may not have provided the information the evaluation team desired, TMA is not aware that a concern of missing information was raised by the team at the time they received the data.

The statement that TMA intends to forgive beneficiary fraud cases involving less than \$25,000 (page 31) is unfounded and incorrect. In fact, the report itself notes (page 30) that the \$25,000 is a DEERS Support Office threshold for referral. TMA Program Integrity has no dollar limit on provider or beneficiary fraud cases it accepts. The only requirement is that it must involve fraud and not a case in which an ID card may have been erroneously issued through no fault of the individual. Fraud cases which are declined for prosecution are referred to the contractors for recoupment, regardless of the dollar amount.

The draft report includes a statement that "in contrast to internal TRICARE procedures, each contractor we visited had a systematic approach to reviewing, documenting and referring ineligible cases and that between April 1 and September 30, 1997, two contractors denied over \$449 million in fraudulent claims from providers, institutions and beneficiaries, \$29 million of which was ineligibility fraud (page 42). Based upon the cases received by TMA Program Integrity and statistical reports provided to us by the contractors, these figures appear inaccurate. Contractors must forward all fraud cases to the TMA Program Integrity Branch. Contractors must also furnish reports that identify fraud and abuse savings. In no single 6-month period were dollars reported that come anywhere close to the amounts quoted in the draft report. Only if we are given information as to the source of this information, can we verify its accuracy.



DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
WASHINGTON NAVY YARD BLDG 111
716 SICARD STREET SE
WASHINGTON DC 20388-5380

5300
Ser 006/9U0016
12 July 1999

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL
(CRIMINAL INVESTIGATIVE POLICY AND OVERSIGHT)

Subj: DRAFT REPORT ON THE EVALUATION OF THE INVESTIGATIVE
ENVIRONMENT IN WHICH THE DEFENSE ENROLLMENT ELIGIBILITY
REPORTING SYSTEM OPERATES (PROJECT NO. 70F-9029)

Ref : (a) DODIG Draft Report dtd June 10, 1999

1. Review of reference (a), disclosed no objection by NCIS to the findings as indicated.
2. The recommendation: The Director, TRICARE Management Activity, to request input from MCIOs to implement a system for developing, referring and tracking cases that involve military health care. It is believed it would be advantageous for NCIS to provide input for the implementation of the recommended system.
3. Should additional information and/or assistance regarding this matter be required, please feel free to contact Joyce Morris at (202)433-9598.

A handwritten signature in black ink, appearing to read "T. W. Fischer", is written over the typed name.

T. W. FISCHER
Assistant Director for Inspections

Copy to:
File

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller/Chief Financial Officer)
Assistant Secretary of Defense (Health Affairs)*
Assistant Secretary of Defense (Legislative Affairs)
Director, Defense Manpower Data Center*

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)*
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)*

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)*

Other Defense Organizations

Director, Defense Criminal Investigative Service*
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Logistics Agency
Director, Defense Security Assistance Agency
Director, National Security Agency
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency

* Recipient of draft report

Non-Defense Federal Organizations and Individuals

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information Technology,
Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations,
Committee on Government Reform